Deleting Personal Data from Vehicles: a GDPR Obligation for Automotive Businesses

Includes the Legal Opinion of Aidan Eardley, King's Counsel (KC)

Sept 2024

PRIVACY4CARS®

privacy4cars.com/gdpr

EXECUTIVE SUMMARY

This whitepaper, *Deleting Personal Data from Vehicles: a GDPR Obligation for Auto Businesses,* provides a detailed analysis by Aidan Eardley, King's Counsel of the London BAR, conducted in May of 2024, clarifying GDPR obligations of automotive-related Controllers, including dealerships, fleet, leasing, motor finance, motor insurance, car rental, carsharing or shared fleet companies, manufacturers, fleet management, and more have in regards to the personal data collected and stored in vehicles (e.g. navigation and smartphone data). It also clarifies the roles and responsibilities of certain Processors, including: motor auctions; vehicle inspection and refurbishment companies; recovery and repossession agents; bodyshop and repairers; recyclers and dismantlers; and more.

Aidan Eardley's KC legal opinion emphasises the importance of understanding data protection responsibilities in the complex ecosystem of vehicle ownership and use, particularly focusing on personal data left on vehicle systems when a business is involved in a vehicle's change of ownership or even just possession, as in the car rental example below:

Aidan Eardley, King's Counsel (KC)

"Upon return of the vehicle, it seems to me, the hiring company will become the Controller of any personal data stored on the vehicle's systems, and the only thing that it can lawfully do with those data is delete them. If it re-lets the vehicle without doing so, such that the next hirer can see the previous hirer's personal data, then there will be a strongly arguable case that the hirer has processed the data in contravention of the Art 5(1) principles."

- Aidan Eardley, King's Counsel of the London BAR, Paragraph 59 of his legal opinion.

This legal opinion and paper should be reviewed by legal counsel in the automotive industry operating in the UK and EU.

The King's Counsel advice is based on data protection law, primarily the Data Protection Act 2018. Since EU GDPR closely aligns with the UK GDPR, and the two laws have identical format, structure, core principles of data protection, and similar rights and obligations for data subjects and data controllers/processors, the King's Counsel opinion has implications for automotive businesses who operate in the European Union and outside of the United Kingdom.

This whitepaper does not constitute legal advice. Our key takeaways after reading the King's Counsel opinion include:

Automotive Business Compliance Obligations:

- Automotive businesses become Controllers[1] of the personal data of prior drivers and passengers under GDPR every time a vehicle returns to their financial or physical control, and is destined to be handed off to a future user or owner (e.g. trade-in, lease return, total loss where systems storing personal data aren't physically destroyed, rental return).

[1] **Controller:** GDPR defines a controller as the 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. Controllers make decisions about processing activities.

- The Controller must delete this personal data. Failing to do so is a potentially reportable data breach (i.e. notification requirements would be triggered). Not deleting the data subjects' personal data from vehicles results in non-compliance with GDPR data protection requirements.
- Controllers cannot shift this legal responsibility to the individuals, whose data was collected, by asking them to delete their own data: GDPR is a consumer protection law and customers or data subjects have no obligations. Any legal language suggesting that customers or data subjects are responsible will not shield businesses from legal responsibility under GDPR and can be considered unfair or deceptive.
- "Best endeavours" are explicitly insufficient for compliance according to the KC opinion. Controllers (or their Processors[2], if a third party is appointed to carry out the data deletion) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance." Controllers are advised to use processes that are objective, repeatable, measurable, and to keep detailed and auditable records.

"A Controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in (UK) GDPR Art 5(2) to demonstrate compliance. A Controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed."

- Aidan Eardley, King's Counsel of the London BAR, Paragraph 22 in his further advice.

Aidan Eardley, King's Counsel (KC)

Liability and Financial Risk to Automotive Companies:

- Controllers may be liable for compensation to customers or data subjects. Legal precedents in similar settings (e.g. personal data left in refurbished electronics) suggest that the mere disregard to have a policy and a process to handle the proper deletion of personal data can result in a claim. Risks for controllers grow with the severity of the data breach and damage the data subject is perceived to have suffered.
- Compensation claims would be handled through civil courts, with each case judged on its merits.
- In the UK specifically, the Information Commissioner's Office (ICO) can investigate complaints, provide enforcement notices, undertake forced inspections and impose penalty fines for serious breaches up to 4% of a company's total global annual turnover. Outside of the UK, Data Protection Authorities (DPAs) play a similar role to the ICO and similarly have the authority to investigate, fine, and take enforcement action against automotive businesses that fail to comply with these provisions.
- Directors and officers may be held personally liable and even face imprisonment in certain situations (e.g. data breaches happening with their consent, connivance, or negligence). The legislation aims not only to punish non-compliance but also to act as a deterrent against lax data security practices.

[2] **Processor:** GDPR defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

- Handing off vehicles (e.g. renting, leasing, selling, etc.) is a core business activity for automotive businesses and not being GDPR compliant may be bring risks beyond the confines of GDPR, especially if companies are public or part of highly regulated industries (e.g. financing, insurance), where material deficiency of internal controls can bring additional levels of scrutiny and exposure.

Best Practices and Next Steps:

- Controllers should have qualified Counsel review this whitepaper and the King's Counsel opinion.
- Controllers should establish a proper in-vehicle personal data deletion policy for the vehicles in their control with demonstrable, appropriate technical and organisational measures. "Best endeavours" are not sufficient. Per the King's Counsel opinion, "A Controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in (UK) GDPR Art 5(2) to demonstrate compliance. A Controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed."
- Should Controllers hire third parties as Processors to meet their data privacy obligations, Controllers are advised to ensure the Processor(s) use proper, objective, repeatable, auditable, and demonstrable processes to delete any personal data from vehicles.
- Controllers should regularly audit and review Processor's data deletion activities, as they will be ultimately responsible for their failures. This is particularly important for those Controllers who have required their Processors to delete the personal data from vehicles but allowed them to do so with a combination of checklists and operators' subjective knowledge - which are proven to deliver inconsistent, sub-par results.
- Processors are advised to notify all the Controllers they serve of the obligation to delete personal data stored in vehicles under GDPR. Processors who offer a data deletion service should ensure the deletion process is robust (i.e. non-subjective) and delivers consistent and auditable results. We included in the Appendix of this whitepaper a template Processors can customise in collaboration with their legal team, to provide notification.
- Controllers should review all customer-facing agreements and privacy notices to reflect their policies regarding the handling of in-vehicle personal data, including how it is deleted. All language or clauses that attempt to assign responsibility to customers or other data subjects should be removed.
- Controllers may need to notify the DPA and any affected individuals about any individual data breach unless a robust policy and process is in place.

In this whitepaper, you will find resources including:

- Information about Privacy4Cars, the world's leading authority on vehicle privacy and data security, which offers data deletion solutions for vehicles.
- A chart outlining the key GDPR data protection roles and responsibilities of automotive businesses.
- Infographics showing the types of data that vehicles collect; the retention of personal data in vehicles constituting the largest unreported GDPR data breach affecting millions annually; how easy it is to re-identify individuals based on personal data found in vehicles; and current unreliable data protection practices of dealerships and wholesalers in the UK.

- The complete, detailed analyses of Aidan Eardley, King's Counsel of the London BAR, outlining how GDPR applies to Controllers in the automotive industry, including: dealerships, leasing, motor finance; car rental; carsharing; or shared fleets; manufacturers; fleet management and applies to Processors; including: motor auctions; inspection and refurbishing; motor insurance; recovery and repossession; bodyshops and repairers; recyclers and dismantlers and more.
- Defining what "best endeavours" means in demonstrating compliance with deleting personal data from vehicles, including using documented procedures and software products designed to remove problematic data.
- Sample letters sent to: associations; dealerships; bodyshops and repairers; motor finance; fleet management; leasing companies; insurance companies; car rental; carsharing; and shared fleets; OEM manufacturers; motor auctions; inspection, refurbishment and storage companies; recovery and repossession agents; and recyclers and dismantlers.
- In Vehicle Data Deletion Process Guidance for Processors and Controllers along with sample policies, disclosure statements, contract addendums outlining controller/processor relationships in the automotive industry in the Appendix including:
    - Appendix 1: Sample Controller Policy and Disclosure Language Covering Personal Data Captured By Vehicles
    - Appendix 2: Sample Disclosure Statement For Processors of In-Vehicle Personal Data To Notify Customers That Are Controllers Of Same
    - Appendix 3: Sample Data Processing Agreement Template UK

Legal disclaimer:

Table of Contents

Table of Contents

ABOUT PRIVACY4CARS

Privacy4Cars – the world's leading authority on vehicle privacy & data security

Privacy4Cars is the first and only technology company focused on identifying and resolving data privacy issues across the automotive ecosystem in the UK, EU, US, and other global automotive markets. Its mission, Driving Privacy, means offering a suite of services to expand protections for individuals and companies alike, by focusing on privacy, safety, security, and compliance.

Enterprise-grade automotive privacy solutions processing millions of vehicles

Privacy4Cars' AutoCleared™ – personal data deletion solution for the automotive industry

Privacy4Cars' personal data deletion solution, AutoCleared™, has been used in millions of vehicles to efficiently manage, execute, and log the deletion of personal data from vehicles – including phone numbers, call logs, location history, garage door codes, and more.

AutoCleared™ delivers objective, repeatable, fast, auditable, and superior data deletion results enabling automotive companies to meet their GDPR compliance requirements. Leading automotive companies – such as dealerships, leasing, motor finance, motor insurance, car rental, carsharing, or shared fleets, fleet management, and more – have used AutoCleared™ for over 2 million vehicles to date, and are able to demonstrate they have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance" - as required by GDPR and other laws.

Privacy4Cars' Vehicle Privacy Report™ – personal data disclosures for the automotive industry

Privacy4Cars' Vehicle Privacy Report™ is a first-of-its-kind solution for privacy disclosures and has been visited over a half million times through pure word of mouth. Its automated privacy labels generate over 10 million impressions a month on dealerships' inventory websites.

Automotive businesses can add 100% automated badges for each vehicle in inventory that links to a branded version of the Vehicle Privacy Report, including disclosures about the data collection and sharing of the manufacturer and key service providers, the compatibility of the vehicle with mobile apps and in-car wi-fi, and credits the business with taking the right steps, including deleting the personal data of prior owners per GDPR obligations.

Award-winning, multi-patented automotive innovations

Privacy4Cars' innovative products have been granted 10 patents and have won or been nominated for auto-industry awards, including:

Automotive WARDSAUTO AutoTech: EUROPE	WINNER: European Start-Up of the Year, 2023
FLEETEUROPE FOR INTERNATIONAL FLEET & MOBILITY LEADERS	FINALIST: Remarketing Innovation of the Year, 2023

The World's Leading Authority on Vehicle Privacy & Data Security. Learn more:
gdpr@privacy4cars.com +44 203 488 4642 https://privacy4cars.com/gdpr

Privacy4Cars, a Sought-After Authority on Automotive Privacy in the Media

With over 1,000 media mentions including: The New York Times; Wired; Times of London; Financial Times; Wall Street Journal; Automotive News; Law360; Bloomberg Law; CNBC; Fleet Europe; Quattroruote; Daily Mail; DarkReading; and more, Privacy4Cars' and its founder, Andrea Amico's analyses and opinions regularly shape the public discourse about vehicle privacy globally.

Learn more about how Privacy4Cars can benefit your automotive business

Learn more about how Privacy4Cars' solutions can benefit your automotive business at privacy4cars.com/about or contact us by phone at +44 203 488 4642 or via email at gdpr@privacy4cars.com.

Data Protection in the Automotive Industry: GDPR Roles & Responsibilities

Automotive Business	GDPR Roles and Responsibilities
Dealerships	Dealers are the **Controller** under GDPR of all personal data stored in vehicles they own. Dealers are mandated to delete personal data from vehicles including: lease returns; trade-ins; dealer-purchased vehicles (wholesale/retail) before they change hands; and courtesy or loan cars after every return.
Leasing	Leasing companies are the **Controller** under GDPR of all personal data stored in vehicles they own. Leasing companies are responsible for deleting, or tasking their 3rd party agents to delete, personal data in vehicles, when the vehicle is returned into their possession and before the vehicle changes hands, including: direct returns or indirect returns (i.e. intermediary) e.g. via collection/inspection agent.
Motor Finance	Motor Finance companies are the **Controller** under GDPR of all personal data stored in vehicles they own. Motor Finance companies are responsible for deleting, or tasking their 3rd party agents to delete, personal data in vehicles, when the vehicle is returned into their possession and before the vehicle changes hands, including: PCP/PCH returns; repossessions and voluntary terminations.
Car Rental, Carsharing or Shared Fleet	Car Rental, Carsharing or Shared Fleet operators are the **Controller** under GDPR of all personal data stored in vehicles they own. Car Rental, Carsharing or Shared Fleet operators are responsible for deleting, or tasking their 3rd party agents to delete, personal data in vehicles, when the vehicle is returned into their possession or between different hirers or users.
OEM (Manufacturers)	OEM (Manufacturers) are the **Controller** under GDPR of all personal data stored in vehicles they own. OEMs (Manufacturers) are responsible for deleting, or tasking their 3rd party agents to delete, personal data in vehicles, when the vehicle is returned into their possession or between different users, including: Demonstration Fleets; Corporate Fleets; Employee Fleets; Press Fleets and Event Fleets.

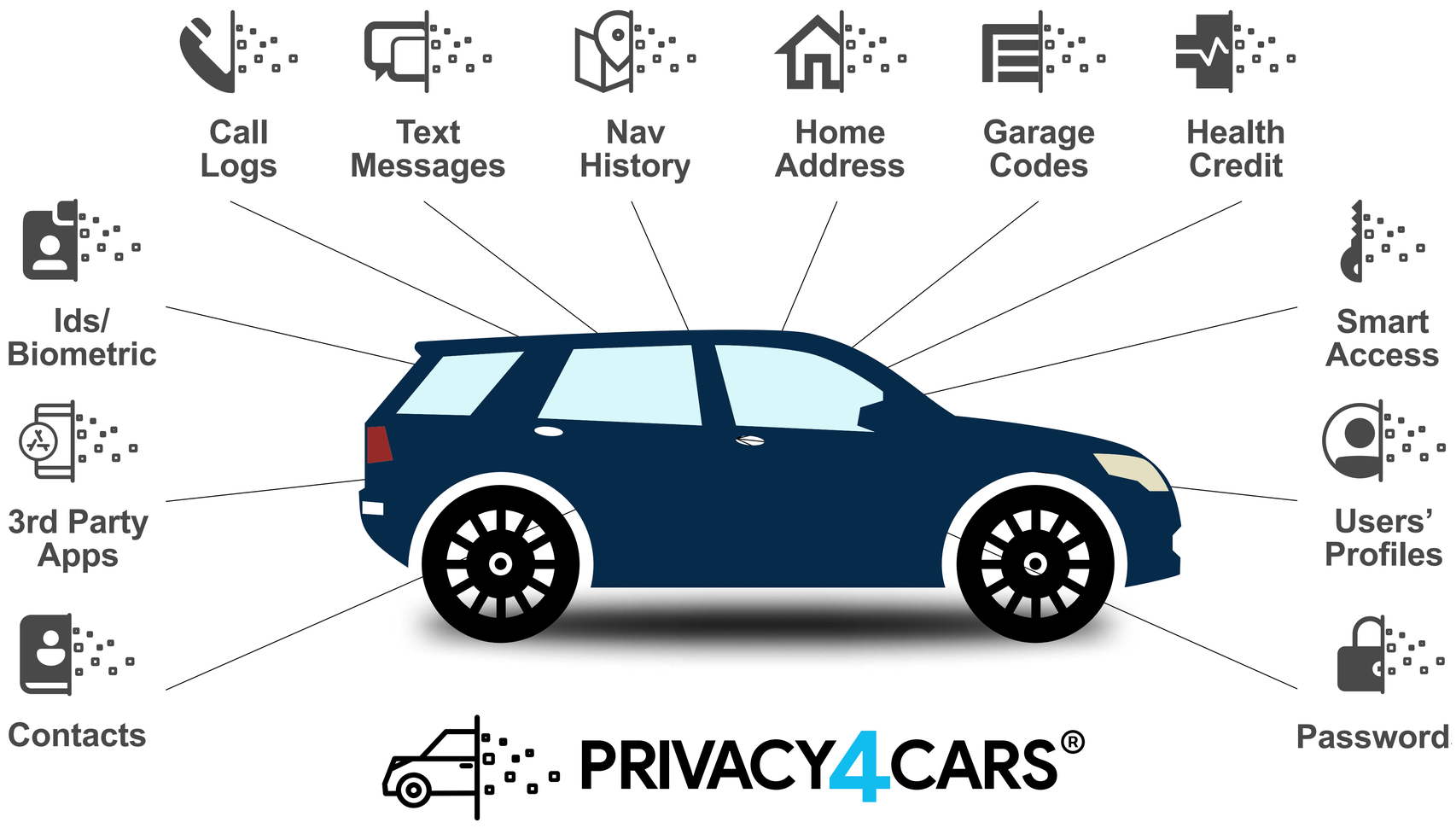
Automotive Business	GDPR Roles and Responsibilities
Fleet	Fleet Management companies are the **Controller** under GDPR of personal data stored in vehicles they own. Fleet Management companies are responsible for deleting, or tasking their 3rd party agents to delete, personal data in vehicles, when the vehicle is returned into their possession and before the vehicle changes hands, including: between different users; and when purchasing or disposing of vehicles directly (e.g. wholesale and retail sales).
Motor Insurance	Motor Insurance companies are the **Controller** under GDPR of all personal data stored in vehicles they gain possession. Motor Insurance companies are responsible for deleting or tasking their 3rd party agents to delete personal data in vehicles when the insurer, or its agent or representative, gains possession of a vehicle e.g. written-off or salvaged to be sold for parts.
Motor Auctions	Under GDPR, Motor Auctions providing inspection, preparation, and remarketing services are considered **Processors** of personal data stored in vehicles they handle. Motor Auctions must notify "without undue delay" all Controllers (clients) of the obligation to delete personal data stored in vehicles to avoid continued data breaches (per Article 33 of UK and EU GDPR). If clients direct them to delete the data, Motor Auctions must do so with consistent, robust, non-subjective, and auditable processes before ownership transfer (best effort and relying on knowledge of employees are not sufficient); If clients do not direct them to do so, Motor Auctions should record the refusal in writing to indemnify themselves from liability. Motor Auctions whose services are limited only to mechanical/ physical/cosmetic matters for a client are considered neither a GDPR Controller or Processor for that client. In this case, Motor Auctions should have a written data processing agreement in place with their client affirming this role.

Automotive Business	GDPR Roles and Responsibilities
Inspection, Refurbishment and Storage Companies	Inspection, Refurbishment and Storage Companies must notify "without undue delay" all Controllers (clients) of the obligation to delete personal data stored in vehicles to avoid continued data breaches (per Article 33 of UK and EU GDPR). If clients direct them to delete the data, Inspection, Refurbishment and Storage Companies must do so with consistent, robust, non-subjective, and auditable processes before ownership transfer (best effort and relying on knowledge of employees are not sufficient); If clients do not direct them to do so, Inspection, Refurbishment and Storage Companies should record the refusal in writing to indemnify themselves from liability. Inspection, Refurbishment and Storage Companies whose services are limited only to mechanical/physical/cosmetic matters are considered neither a GDPR Controller or Processor. In this case, Inspection, Refurbishment and Storage Companies should have a written data processing agreement in place with their client affirming this role.
Recovery & Repossession Agents	Recovery & Repossession Agents have no responsibility under GDPR, unless instructed by their client to delete personal data from a vehicle, where they become GDPR Processors. If clients direct them to delete the data, Recovery & Repossession Agents must do so with consistent, robust, non-subjective, and auditable processes before ownership transfer (best effort and relying on knowledge of employees are not sufficient) and to have a written data processing agreement in place with their Client.

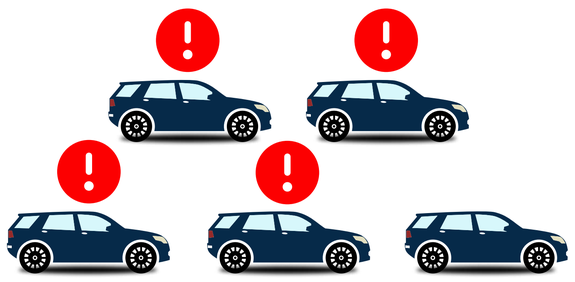
Automotive Business	GDPR Roles and Responsibilities
Bodyshops and Repairers	Bodyshops and Repairers that service vehicles owned by clients have no responsibility under GDPR, unless instructed by their client to delete personal data from a vehicle, where they become GDPR Processors. If during the service the Bodyshops or Repairers become aware of a likely change of ownership (e.g. a vehicle is written off for salvage), they must notify the Controller (e.g. the insurance company) of their responsibility to delete the data under GDPR (similar to inspection companies), and if the Controller agrees, they become Processors. If Controllers do not direct them to do so, Bodyshops and Repairers should record the refusal in writing to indemnify themselves from liability. Bodyshops and Repairers are a GDPR Controller and are responsible for deleting personal data in vehicles when managing courtesy, loan cars, or similar owned or otherwise controlled by their business Whenever a Bodyshop is a Processor or a Controller, they must delete personal data with consistent, robust, non-subjective, and auditable processes before ownership transfer (best effort and relying on knowledge of employees are not sufficient) and to have a written data processing agreement in place with their client.
Recyclers and Dismantlers	Recyclers and Dismantlers have no responsibility under GDPR, unless instructed by their client to delete personal data from a vehicle or its component parts, where they become GDPR Processors. When Recyclers and Dismantlers serve as Processors, they must delete personal data with consistent, robust, non-subjective, and auditable processes before ownership transfer (best effort and relying on knowledge of employees are not sufficient) and to have a written data processing agreement in place with their client.

INFOGRAPHICS

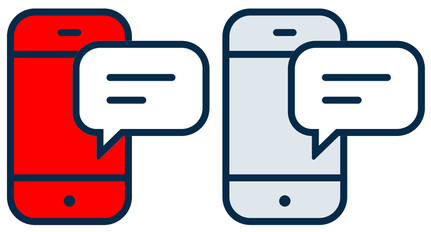
Vehicles collect lots of personal data that must be deleted when changing hands by GDPR-regulated businesses.



Personal data is regularly left in vehicles, making it the largest unreported GDPR data breach, affecting millions each year.



4 out of 5 vehicles are resold with personal data*



1 out of 2 customers find stored phone info (calls, texts, etc.) in vehicles for sale**

1 out of 3 customers find stored home addresses/ locations in vehicles for sale**

* **Source:** Privacy4Cars sample of hundreds of vehicles for sale at retail and wholesale locations, UK, Germany, Italy. 2021-2024

** **Source:** Privacy4Cars mystery shopper audit of pre-owned vehicles for sale at 46 leading UK dealerships, Dec 2023-May 2024

The World's Leading Authority on Vehicle Privacy & Data Security. Learn more:

gdpr@privacy4cars.com +44 203 488 4642 https://privacy4cars.com/gdpr

Companies that don't include vehicles in their device management policies risk exposing information about their companies.

A pharma rep's fleet vehicle revealed cancer trial patients' addresses & more via the vehicle's stored text messages	**A crashed car exposed a bank VP's identity, passwords, & sensitive personal information of other execs including CEO, CFO, & GC**	**An actor's former sports car retained garage codes to his mansion**	**A luxury vehicle of a celebrity revealed her private residence, two direct phone numbers, and personal data**

Additional data exposure risks can include family details, children's schools, and places of worship. Financial data like credit card records and banking PINs. And service accounts, browsing histories, medical information, and more.

Source: Research by Privacy4Cars

Re-identifying company data - including information about suppliers, affiliates, employees, & their families - is incredibly easy.

An ex-fleet vehicle for sale easily revealed the identity of a military contractor with security clearance, restricted access and classified sites, other business and personal data.

PRIVACY4CARS®

Full Name lives in Hereford at Exact Address

His smartphone data such as contacts, call history, messages, and personal email was stored in the vehicle, including his work email.

He works for Military Contractor and specialises in military telecom systems and biometrics.

Has top level security clearance and his common destinations include several military research locations.

He works with the Navy Command HQ in Portsmouth, Military Contractor in Malvern, a company specialising in "air, land, and sea tactical system training and testing", and at the HQ of Military Contractor.

He visited the UK Army Cadet HQ.

He visited a *reportedly decommissioned* telecommunications and fiber facility.

He has a second/holiday home at Exact Address.

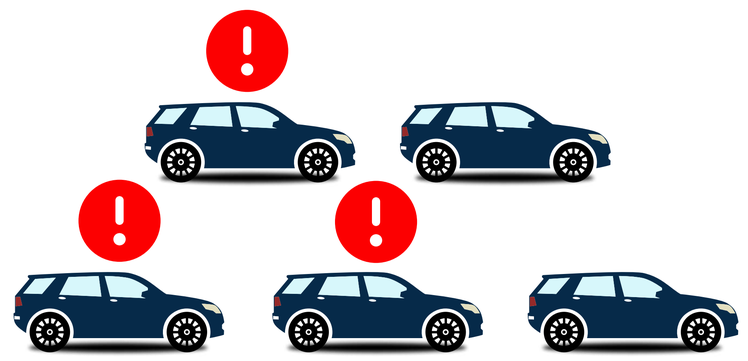
He enjoys watching a game of cricket and going ice skating.

Source: Analysis by Privacy4Cars of a ex-fleet vehicle for sale in the UK, 2022

PRIVACY4CARS®

3 out of 5 times, dealerships break their promise
to delete customer data, despite GDPR requirements, due to not using robust, repeatable, & non subjective deletion methods.

3 out of 4 dealers tell customers they always delete personal data from used vehicles for sale



Yet, at those dealerships that promise data deletion is a standard of care, customers find personal data in 3 out of 5 test drives

Source: Privacy4Cars Mystery Shopper Audit at 46 leading UK dealerships, Dec 2023-May 2024;
Out of 46 dealers, 35 represented to always delete personal data; customers found data in 40 out of 70 test drives at those dealerships. 3 dealerships said they delete the data upon request; 8 did not clearly answer.

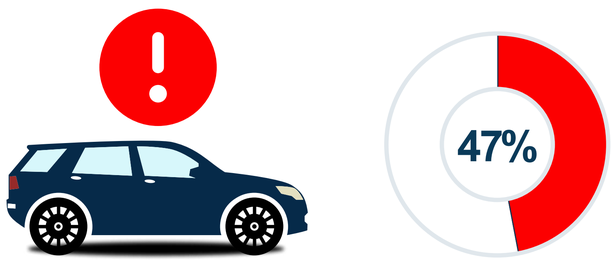
Subjective Knowledge for Data Deletion is Unreliable
and Controllers should audit deletion results to ensure Processors do not overrepresent their capabilities when not backed by tools.

Controller: OEM captive (2 makes, 6-36 month old vehicles)

Processor: Inspection Company

Method: added a “Personal Data deleted” checkbox to their standard Condition Report; ***rely on inspector experience (no tools)***

Result: by using a sub-par service and not auditing their Processor, Controllers' customers frequently experienced a data breach

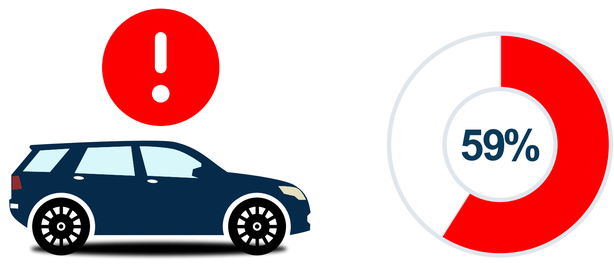


Controller: UK Online retailer (various makes, 12-36 month old)

Processor: Motor Auction

Method: Personal Data deletion is part of the standard vehicle prep checklist; ***rely on personnel experience (no tools)***

Result: by using a sub-par service and not auditing their Processor, Controllers' customers frequently experienced a data breach



Controllers should refuse to accept data deletion processes based on checklists and Processors’ subjective experience and imagination. “A Controller who uses [...] a software product designed to remove problematic data will be much better placed” to comply with GDPR.

Aidan Eardley, King’s Counsel (KC)

Source: Privacy4Cars audit at two UK facilities, 2022-2023

The World's Leading Authority on Vehicle Privacy & Data Security. Learn more:

gdpr@privacy4cars.com +44 203 488 4642 https://privacy4cars.com/gdpr

Analyses by Aidan Eardley, King's Counsel (KC) Clarifying the GDPR Obligations of Automotive-Related Businesses

Foreword

In the following section, we provide two analyses by Aidan Eardley, King's Counsel (KC) clarifying GDPR obligations of automotive-related businesses. **This legal opinion and paper should be reviewed by legal counsel in the automotive industry operating in the UK and EU.**

The first analysis, conducted on 15 May 2024, clarifies the GDPR obligations of automotive-related Controllers, including: dealerships; fleet; leasing; motor finance; motor insurance; car rental; carsharing or shared fleet companies; manufacturers; fleet management; and more have in regards to the personal data collected and stored in vehicles (e.g., navigation and smartphone data). It also clarifies the roles and responsibilities of certain Processors, including motor auctions, vehicle inspection and refurbishment companies, recovery and repossession agents, bodyshop and repairers, recyclers and dismantlers, and more. A key takeaway from the analysis is described in the car rental example below:

> *"Upon return of the vehicle, it seems to me, the hiring company will become the Controller of any personal data stored on the vehicle's systems, and the only thing that it can lawfully do with those data is delete them. If it re-lets the vehicle without doing so, such that the next hirer can see the previous hirer's personal data, then there will be a strongly arguable case that the hirer has processed the data in contravention of the Art 5(1) principles."*
>
> *- Aidan Eardley, King's Counsel of the London BAR*

The second analysis, conducted on 2 September 2024, provides further advice discussing the broader applicability of the analysis to the EU and the organisational requirements to demonstrate compliance. A key takeaway from the analysis is:

> *"A Controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in (UK) GDPR Art 5(2) to demonstrate compliance. A Controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed."*
>
> *- Aidan Eardley, King's Counsel of the London BAR*

The Full Legal Opinion by Aidan Eardley, King's Counsel

AIDAN EARDLEY KC OPINION

In the matter of AutoTek21 Ltd

ADVICE

Introduction

1. I am asked to advise AutoTek21 Ltd on the responsibility, under UK data protection law, for personal data that is left on the on-board computer of a vehicle by its user when that vehicle changes hands. A number of different factual scenarios which commonly arise in the automotive industry have been set out for my consideration.
2. I have taken into account all the written materials supplied with my instructions and also the helpful information that I was given on a call with my clients on 29 April 2024. I had a further call, and received further information by email, after circulating a draft of this advice and I have expanded the advice to cover some additional points that were raised. I advise in relation to the legal position in England and Wales.

Summary of advice

3. In summary, I advise as follows:

(1) Ordinarily, once full control over a vehicle is transferred/returned to an entity such as a long-term lessor, a finance house, insurer, or a short-term hire company, that entity will most likely be regarded as the controller of any personal data stored on the vehicle's on-board computer system. That will likely be the case even where the lessor (etc) has told the user of the vehicle to delete data prior to handing it over. For short-term hire companies, that will be the case at the end of each short-term let;

(2) Intermediaries who are involved in recovering the vehicle, storing it, inspecting it or refurbishing it prior to it being remarketed may have no liability in data protection law whatsoever, or they may be "processors" acting on behalf of the lessor (etc). That will depend on the precise nature of their role. It is highly unlikely that any such intermediary would be classified as a controller of the data held on the vehicle's system;

(3) Where the vehicle is resold via an auction house, the auction house will typically not have any liability in data protection law or, at most (if e.g. it undertakes to inspect and warrant the condition of the vehicle), it will be a processor acting on behalf of the seller. The position of other reselling agents will need to be considered on a case-by-case basis;

(4) Dealers who hold or acquire vehicles are likely to be either controllers or processors, depending on the precise circumstances. If they straightforwardly buy a car from an individual with a view to reselling it, they will be the controller. If they receive the car on behalf of a finance house, without buying it, they will not be the controller but may be the processor, depending on what the finance house requires them to do with the vehicle. If they provide courtesy cars or test drives, they are likely to be the controller of any information left on the car's system once it is returned.

(5) It follows that, ordinarily, the lessor/finance house/hire company (and sometimes the dealer) that takes possession of the vehicle will be under a duty to delete any personal data stored on its on-board computer. That will usually be the only lawful processing operation that could be undertaken in the circumstances.

(6) A lessor (etc) who does not delete the data before reselling the vehicle will be at risk of a claim for compensation. It is highly unlikely that they could avoid liability by blaming the user of the vehicle for failing to remove the data before returning it. It is possible that the compensation payable might be reduced in such circumstances on the basis of contributory negligence.

Definitions and concepts

4. The principal source of data protection law in the UK is now the **UK GDPR** (a slightly modified version of the EU GDPR) supplemented in some respects by the Data Protection Act 2018 (**DPA 2018**).

Processing

5. The UK GDPR concerns the "processing" of personal data. Not all "processing" is included within the scope of the legislation. Purely manual processing is largely excluded as is, importantly, "*the processing of personal data by an individual in the course of a purely personal or household activity*", whether manual or automated Art 2(2)(a). "Processing" however, has an extremely wide definition. Art 4(2) provides:

   "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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."

6. "Storage" is regarded in the authorities as a continuing act of processing, not just the initial act by which information is entered into a device, see *Buivids* [2019] 1 WLR 4225 at [33]-[36] (preservation of a recording in the memory of a digital camera). Thus the continued presence of data on a device such as an on-board computer in a car will, it seems, count as processing, for which someone may be responsible, at least where the device is still functional.

7. There is a question as to whether an act of processing (although it literally falls within the very broad definition in the UK GDPR) can be disregarded as trivial. Nicklin J appears to have thought so in the recent case of *Farley v Paymaster (1836) Ltd* [2024] EWHC 383 at [146], where he held that the sending of a letter containing personal data, which was not opened and read, did not involve any "real processing". That decision is highly contestable in my view, although questions about the *de minimis* principle arise again later in the analysis, when one considers (for the purposes of Art 82) what counts as an "infringement" and what counts as compensable "damage". They are highly pertinent here because, where personal data are left on a vehicle's system, the next user of the vehicle will often just ignore them, perhaps being slightly irritated by their presence.

8. There could of course be much more damaging consequences for a data subject whose data are left on a vehicle's systems. My clients have informed me anecdotally of cases where, e.g. a new owner of the vehicle tracks down and confronts a previous owner, or stalks them, or where they (deliberately or inadvertently) use the previous owner's financial details stored in an on-board app to make purchases (e.g. when paying to recharge the battery).

Controllers and Processors

9. Principal responsibility for any particular act of processing lies with the "controller", defined in Art 4(7) as "*the 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 …"*. The term is interpreted expansively, so as to ensure the "*effective and complete protection of data subjects"* [1].

10. There is guidance from both the ICO and the European Data Protection Board (**EDPB**) on how to identify the controller. To summarise, one is looking for the person (or persons) who decides on the key elements of the processing operation (the, "what", "why" and the "how"). This is a functional test, to be applied in all the circumstances: in other words, one looks at the factual situation. The contractual terms between parties may assist in identifying which of them is a controller, but cannot be determinative: a party cannot contract out of their obligations as a controller if, as a matter of reality, it is they who are calling the shots as to what processing is undertaken[2]. Similarly, it seems clear to me, whether someone has legal ownership, or physical custody, of a device that contains personal data may be informative as to whether they are a controller of those data, but not necessarily conclusive. Likewise, whether someone is the registered keeper of a vehicle (or should register themselves as the keeper) is likely to be indicative of controller status (since it implies responsibility for the vehicle itself in a number of legal contexts) but not necessarily conclusive.

11. A controller will normally actively turn their mind to the question of what personal data they are collecting, storing etc, how they are doing so and why. However, it seems to me that a person will be a controller even if they are indifferent to whether processing is occurring, or it occurs incidentally in the course of their main activities, so long as it is they, and not someone else, who are in a position to make the key decisions about the processing. The EDPB Guidelines, at [44], state "*Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a "controller" even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data*".

12. Also, it is not essential that the controller actually has access to the person data that is being processed. Thus, in *Wirtschaftsakademie Schleswig-Holstein* [2019] 1 WLR 119, the administrator of a Facebook fan page was (along with Facebook itself) the controller in respect of the collection of personal data about visitors to the page (having given Facebook instructions about the sort of information it was interested in) even though the personal data were collected only by Facebook and not passed on in identifiable form. Likewise, in *Jehovan todisajat* [2019] 4 WLR 1, individual Jehovah's witnesses (who were uncontroversially controllers in their own right) collected personal data about the individuals they met on the doorstep in the course of their preaching activities, but the central Jehovah's witness organisation (which did not usually receive any of the data) was also held to be a controller because it engaged in "*organising, co-ordinating and encouraging*" the preaching activities of its members.

13. Academic commentary (so far not confirmed in case law or guidance) suggests that "data subject" and "controller" are mutually exclusive terms so that, rather paradoxically, where a data subject records information solely about themselves[3], there may be no controller in the picture.

[1] Google Spain [2014] QB 1022, at [34].
[2] See e.g. EDPB Guidelines 07/2020 at [28].
[3] At least on a standalone device. Writing about oneself on Facebook etc is likely to involve at least some processing that is under the control of the social media platform.

14. “Controller” is also defined in contradistinction to a “processor”, that is, “*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*”: Art 4(8). A processor has some scope to determine how it goes about the processing (particularly at a technical or operational level) without rendering itself a controller, so long as the essential decision making about the purpose and means of the processing rests with the entity that engages the processor. Processing by a processor is only lawful if done on the authority of the controller and pursuant to a written processor controller agreement (Arts 28 & 29).

15. Importantly, the EDPB Guidelines also recognise a third category of person: someone who may come into contact with, or even process, personal data, but in such an accidental or incidental way that they are neither a controller nor a processor. One example given (at [83]) is an IT consultant who is engaged by a controller to fix a software bug. He is not hired to process personal data but may incidentally come across some as he goes about his work. The EDPB’s analysis in this situation is that responsibility remains with the controller, who must, pursuant to the security principle (Art 5(1)(f) and Art 32) take appropriate steps to prevent the consultant from processing personal data in an unauthorised manner.

16. Another example, at [88] in the Guidelines, is a cleaning company, engaged to clean the company’s offices, but prohibited from accessing personal data on the controller’s systems. The fact that cleaners may occasionally come across personal data as they clean would not be enough to render the cleaning company either a controller or processor. This is clearly a question of fact and degree: see the contrasting example, at [83], of a company engaged to provide general support on the controller’s IT systems which store a large volume of personal data. The Guidelines say, “*The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing this service*”, rendering the service provider a processor for GDPR purposes.

The Data protection principles

17. UK GDPR Art 5(1) sets out six principles governing the processing of personal data. Art 5(2) provides that it is the controller who is responsible for, and must be able to demonstrate, compliance with the principles. For present purposes, the following principles are particularly pertinent:

    1. Personal data shall be:

        (a) Processed lawfully, fairly and in a transparent manner…

        (b) […]

        (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ...

        (d) […]

        (e) […]

        (f) Processed in a manner that ensures appropriate security of the personal data, including protectionagainst unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures …

18. UK GDPR Art 32 expands on Art 5(1)(f), and importantly places a free-standing obligation on a processor. It provides that “*the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…”* [i.e. the risk to the interests of individual data subjects].

19. Art 5(1)(f) and Art 32 provide a certain degree of latitude to controllers and processors. Their duty is not to prevent unauthorised processing (etc) at all costs, only to take "appropriate" measures to guard against the risks involved. In the context of cybersecurity, the CJEU has confirmed that the fact that hacking has occurred is insufficient: the question will always be whether the controller took precautions that were commensurate with the risk[4]. This has some significance here since, as mentioned above, personal data left on a vehicle's systems is often likely to be of no interest to the next owner/driver and probably just a source of irritation. Controllers and processors (whoever they may be: see below) might seek to argue that, in those circumstances, the "appropriate" measures are fairly limited, and that requiring the previous user of the car to delete data, together with, perhaps, a cursory and superficial inspection of the on-board computer, would suffice. Nevertheless, as noted above, there is certainly scope for the data left on a vehicle to be abused by a subsequent owner, causing the data subject great detriment, so a more thorough process of inspection and erasure is probably in order. Further and in any event, the other principles do not afford a controller similar "wiggle room". If there is no legal basis for processing, there will straightforwardly be a breach of Art 5(1)(a). And if a controller retains data when they are no longer needed, there will be a breach of Art 5(1)(c), and that will be so even if the controller has made some ineffective effort to remove them.

Personal data breach

20. A "personal data breach" is defined in Art 4(12) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The term is sometimes used (including by the ICO) to cover any sort of unlawful processing but, properly construed, it is limited in my view to situations where there has been a breach, or an arguable breach of Art 5(1)(f) and/or Art 32. The particular significance of classifying an event as a "personal data breach" is that it triggers reporting obligations (to the ICO and data subjects) under Arts 33 and 34 (see further below).

Compensation

21. Art 82 determines the liability of controllers or processors to pay compensation when there has been an infringement of the GDPR. It provides:

    1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
    2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
    3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
    4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

[4] See e.g. Natsionalna agentsia za prihodite C-340/21, 14.12.23

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

22. “Damage” includes both financial harm (pecuniary damage) and any distress a data subject may suffer (non-pecuniary damage). There is debate about whether it extends to mere “loss of control” over personal data, but it is unnecessary to examine that here because, in the scenarios we are considering, a data subject who complains that their data have been left on a vehicle’s system is likely, at the very least, to assert that they have suffered distress.

    The CJEU has held that compensation for non-pecuniary damage will be due where a data subject experiences a well-founded fear that their data will be misused by a third party to whom they have been disclosed. Before a fear is “well—founded” it will be necessary for the data subject to show that a third party has actually become aware of the data. A purely hypothetical risk will be insufficient[5].

23. There is also a debate about whether the “infringement” or the damage caused by it, must surpass a certain level of seriousness before it can give rise to liability. The Supreme Court said “yes”, in *Lloyd v Google* [2022] AC 1217 (considering the position under the Data Protection Act 1998). The CJEU appears to have said “no” in *Osterreichische Post AG* (C300/21, judgement of 04.05.23) (a post-Brexit case and so not binding on UK courts). In *Farley* Nicklin J considered the point to be open as a matter of domestic law. Meanwhile, UK courts have made robust use of their case-management powers in low value data protection claims, often transferring them to the County Court and either directing or encouraging that they should be allocated to the small claims track, where a claimant cannot usually recover their costs: see e.g. *Cleary v Marston (Holdings) Ltd* [2022] Costs L.R. 1451. The requirement that any fear of misuse of personal data by a third party must be “well-founded” as opposed to hypothetical may, in practice, serve to exclude trivial claims.

24. It is clear from the terms of Art 82 that there is no need to prove negligence on the part of the controller or processor in order to recover compensation: upon proof of unlawful processing causing damage there is a presumptive right to obtain compensation from each controller (and in some cases, processor) “involved” in the processing. The only way such a controller or processor can avoid liability altogether is by proving that it is “not in any way responsible” (so, “best endeavours” etc will not be good enough). Unless they can surmount this high hurdle, the best an infringing controller or processor can do (within the terms of Art 82 itself) is look around for another guilty controller/processor and seek a contribution from them (Art 82(5)).

25. A question arises as to whether English law principles of contributory negligence can be relied on to reduce compensation otherwise payable under Art 82, for example where a car hire company or similar had told the user to delete their data before returning the vehicle and, having failed to do so, the user then sues the company in respect of the disclosure of their data to subsequent hirers of the vehicle. The Law Reform (Contributory Negligence) 1945 Act s1(1) relevantly provides:

    “Where any person suffers damage as the result partial of his own fault and party of the fault of any other person or persons, a claim in respect of that damage shall not be defeated by reason of the fault of the person suffering the damage, but the damages recoverable in respect thereof shall be reduced to such extent as the court thinks just and equitable having regard to the claimant’s share in the responsibility for the damage…”

[5] BL v MediaMarktSaturn Hagen-Iserlohn GmbH C-687/21, 25 January 2024 (another post-Brexit case, so persuasive rather than binding in the UK)

26. Until very recently, the answer to this question would have been a clear “no”. Art 82 is a self-contained provision about how questions of compensation should be approached under the UK GDPR and it does not provide for any reduction in compensation on the basis of fault by the data subject. As a provision of “retained EU law”, it took precedence over any conflicting domestic law principles, such as the 1945 Act.

27. The Retained EU Law (Revocation and Reform) Act 2023, which came into force in January 2024 and amended the European Union (Withdrawal) Act 2018 (EUWA) has changed all this: the principle of the supremacy of EU law has been removed; “assimilated direct legislation” (as it is now termed) such as the UK GDPR, must “so far as possible” be read and given effect in a way which is compatible with all domestic enactments and, if that cannot be achieved, the domestic enactment takes precedence: EUWA s5[6].

28. Accordingly, it seems to me that a controller or processor, who is prima facie liable to pay compensation under Art 82 to the previous user of a vehicle, might well be able to argue for a reduction in the amount payable on the basis of the 1945 Act where the user had been asked to, but failed, to delete their data. I should stress however that this is a complex and presently untested argument.

Specific guidance and case law

29. The questions raised by my instructions have not been definitively addressed in guidance or case law.

30. As to sector-specific *guidance, the EDPB produced “Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*” (09.03.21). The main focus of those guidelines however is the situation in which a vehicle transmits information (e.g. about location, maintenance, driving style etc) to a manufacturer, insurer or such like. The guidelines do acknowledge that drivers and passengers will create records of personal data on the in-car system, e.g. by entering satnav directions, pairing a phone by Bluetooth etc. The view taken is that, where this is done without the data being transferred to a controller or processor elsewhere, the processing will occur in the course “of a purely personal or household activity” and will therefore be outside the scope of the GDPR: see [73]-[74]. Also, at [92], the guidelines state “*The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes …*” but is frustratingly silent as to who has this duty to delete: the user parting with the car; the next registered owner; someone else in the chain between these two? I give my own views on these questions below.

[6] There is a carve out for some aspects of data protection law (see s5(A3)) but it does not cover domestic legislation, such as the 1945 Act, that might limit entitlement to damages.

31. As to case law, some inconclusive assistance can be gained from Stadler v Currys [2022] EWHC 160. There, a customer returned a faulty smart TV to Currys, on which he had used various apps, including Amazon Prime. Currys considered that it was uneconomical to repair the TV so offered to write it off and give the claimant a voucher to purchase a new TV. Currys however did not destroy the TV; they re-sold it (to a company), and without first doing a factory reset. The TV was sold on and the eventual new owner then used the claimant's Amazon app (he had not logged out) to purchase a movie. The claimant sued Currys, including under data protection law, alleging that Currys was a controller in respect of his personal data that had been stored on the TV. Curry's argued that it had only ever held the TV as a physical asset, did not make use of any of the claimant's data and was unaware that the data was on the TV, asserting in those circumstances that it could not be a controller and did not process the data. HHJ Lewis refused to strike out the claim, saying, at [33]*"On the basis of the claimant's account of events, it seems that the defendant would or should have been aware that there was personal data on the device, and it is certainly arguable that it had duties as a data controller particularly if at any point it became the owner of the Smart TV…". Stadler* therefore gives at least some indication that a person becomes subject to the duties of a controller in respect of data stored on a device when they acquire ownership or physical possession of it. There are no further reported decisions in the *Stadler* litigation and I suspect that it was settled after being transferred to the County Court.

32. *Stadler* also mentions at [27] a decision in a German local court, where a company was ordered to pay damages when they re-sold a damaged computer, having refurbished it but without removing the claimant's personal data from the hard drive. The company had told him to do this himself before returning the machine[7]. The court held that by selling the machine on, the company unlawfully disclosed the claimant's personal data to the purchaser. The company was not permitted to rely on its instruction to the claimant to delete his own data, which would have amounted to a blanket exclusion of liability. Neither could it avoid liability for damages in reliance on Art 82(3), since it had intended to remove the data and had failed to do so through the human error of an employee. The claimant was awarded €800 damages for distress.

The four scenarios

Scenario A - "Leasing and Contract Hire Agreements"

33. In this scenario, the legal owner of the vehicle (**lessor**) grants a long lease to a user (**lessee**). At the end of the lease, the lessor recovers the vehicle, inspects it, refurbishes it, and then sells it on. Although the lessor could do all these things itself, it will typically use a number of middlemen, viz, a logistics company to collect the vehicle from the lessee; a company to carry out the inspection and refurbishment, and a reselling agent such as an auction house. There may be other intermediaries involved as well, e.g. a company that provides physical storage of the vehicle. The lessor itself may never actually regain physical custody of the vehicle as it goes through the process.

34. On our call, I was told that the [Company A] scheme is a prime example of this type of arrangement and that [Company B] are another example of a company acting as a lessor. The [Company B] vehicle return guide I have been sent contemplates that the lessee will have been the registered keeper of the vehicle during the lease and that registration will then be transferred back to the lessor at the end of the lease (see p.9). The guide (p.10) requires the lessee to remove all personal data from the vehicle before surrendering it. The lessee will be the registered keeper during the lease but this will cease when the lease comes to an end. The [Company A] documentation I have seen is silent on the question of removing personal data at the end of the lease.

[7] AG Hildesheim, Urteil vom 05.10.2020 – 43 C 145/19 (dsgvo-schmerzensgelder.de)

35. Dealing first with the position of the lessee. They will have stored personal data on the vehicle's systems during the currency of the lease. If it is correct that a person cannot be both data subject and controller in respect of the same information, they will never have been a controller in respect of their own personal data stored on the systems. Insofar as they stored the data of others (e.g. phone numbers and addresses of friends and family) they will have been the controller in respect of that processing but would not be subject to the UK GDPR because this will have been processing done "by an individual in the course of a purely personal and household activity". However, when the vehicle is handed back to the lessor (or its agents), that may well be regarded as an act of processing, in that it consisted in the transmission of the data still stored in the vehicle[8] and arguably one that fell outside the "purely personal and household activity" exclusion, since the lessee is handing the vehicle back pursuant to a commercial agreement. So, in principle, a friend or family member of the lessee whose data was transferred in this way could seek compensation from the lessee in the event that they suffered material or non-material damage.

36. Turning then to the lessor, in my view there is a very strong case that, at the point when the lease comes to an end, and the lessor regains full rights over the vehicle, they become the controller in respect of any personal data stored on the vehicle's systems. At that point, the lessor is in a position to decide what should be done with the data; it can decide upon a purpose for retaining/disclosing/deleting the data; and it can decide how that purpose should be achieved. These are the classic indicia of "controllership" in data protection law. The lessor may never take physical possession of the vehicle (and so may never be in a position to actually access the data), and it may be (and probably is) entirely indifferent about what data is on the system. However, the principles and guidance I have summarised above indicate that these matters are not determinative.

37. The dicta in *Stadler* support this analysis, suggesting that, ordinarily, assumption of legal and physical control over a device also entails assumption of controllership in data protection law. There may be exceptions, e.g. where the device is so damaged that the data are irretrievable by ordinary means (in which case, query whether they are still "stored" at all), or where they are securely encrypted (in which case, the acquiring party could not exercise any effective control over them), but these will not occur in most run-of-the-mill cases.

38. There is a narrower view, namely that a person only becomes the controller of the data stored on a device they receive once they actively start to inspect the device. That would be consistent with the facts in *Stadler* and the German case (where, in both instances, the defendants had fired up the devices in order to restore functionality and prepare them for resale). It is difficult to reconcile, however, with the fact that processing is defined as including "storage".

[8] See, by analogy, Satamedia C-73/07, CJEU Grand Chamber, 16.12.08) at [37]. Provision of a CD-ROM by one controller to another was held to amounted to the transfer and hence processing of the personal data on the CD

39. Assuming my analysis is correct then, upon the vehicle being recovered from the lessee, the lessor becomes the controller in respect of the personal data stored on the vehicle's systems. Contractual provisions stipulating that the data remain the responsibility of the lessee will not prevent that conclusion, because they do not reflect the reality of the situation. Any processing must have a lawful basis under UK GDPR Art 6. Upon initially regaining full rights over the vehicle, Art 6(1)(b) will usually apply ("processing is necessary for the performance of a contract to which the data subject is a party"). There will be a contractual obligation on the lessor to accept the return of the vehicle and, if that cannot be done without also acquiring responsibility in data protection law for storage of the personal data on the vehicle's systems, then there will be lawful processing at the point of return. In my view however, that legal basis will be short-lived – just long enough to give the lessor a reasonable opportunity to have the data wiped. It is certainly not capable of covering the processing that will (probably) occur when the vehicle is sold on to a new owner.

40. In reality, therefore, a lessor is obliged to delete all personal data from a vehicle's on-board computer when the lease comes to an end. Failing to do so effectively may place the lessor in breach of Art 5(1)(f) and Art 32 (depending whether the efforts they took to remove the data amounted to "appropriate" security measures). But in any event (and regardless of whether the lessor has used their "best endeavours"), handing on the vehicle with the data still intact is likely to breach both of Art 5(1)(a) (lawfulness) and Art 5(1)(c) (data minimisation).

41. The lessor will therefore be at risk of having to pay compensation pursuant to Art 82(2) where the failure to remove the data has caused a data subject pecuniary damage or non pecuniary damage (i.e. distress). It seems unlikely that Art 82(3) would assist in most cases. A lease agreement might require strong and explicit warranties from the lessee that they will remove all personal data from the vehicle at the end of the lease but, even then, the lessor will have had an opportunity to check whether the lessee had complied. If the lessor sells a vehicle onwards without having undertaken that check, it will be difficult for it to discharge the burden of proving that it is "not in any way responsible for the event giving rise to the damage".

42. Where the claim for compensation comes from the lessee themselves (complaining that their own data has been left on the vehicle), and the lessee had been required under the terms of the lease to remove their data, then it may be possible for the lessor to invoke the principle of contributory negligence to reduce the amount of compensation they must pay. That will depend on the (as yet untested) proposition that Art 82 must now be read subject to the 1945 Act.

43. Where the claim for compensation comes from another data subject (e.g. a friend or family member of the lessee whose data have been stored on the system) the lessor could try to seek a contribution from the lessee under Art 82(5) because, in that situation, the lessee will probably have acted as a controller in respect of those data when returning the vehicle and so could be said to have been infringed the UK GDPR themselves, and to have been involved in the processing that led to the damage. However, it will often be impractical and uneconomic for the lessor to pursue the lessee, who may well be a private individual of limited means.

44. I would add that an insurer who writes off an insured vehicle and then gains possession of it (directly or through agents) so that it can be sold for parts, will be in an analogous position to a lessor who gains control over the vehicle at the end of the lease, and will therefore be under the same duties to delete personal data left on the vehicle's systems (assuming that the systems are still operable).

45. I turn next to the various middlemen who may be involved, on behalf of the lessor, in collecting the vehicle, storing it, inspecting it, and preparing it for onward sale.

46. As I understand it, these intermediaries will be engaged and paid by the lessor, essentially to perform tasks that the lessor would need to do itself, but which it is more economical to contract out to third parties. It is therefore highly unlikely that any of these intermediaries would be regarded as controllers: they will be acting pursuant to narrowly circumscribed instructions (deliver the car here; do this 100-point inspection etc); they are unlikely to have the latitude to make decisions about the "what, how, why" of any processing they may engage in.

47. In terms of analysis of these intermediaries therefore, the choice is between "processor" and that third category of entity recognised by the EDPB who is neither a controller or processor. This will depend on what the intermediary is tasked to do, and the extent to which the processing of personal data might be said to be integral to that role.

48. In the case of intermediaries who simply move the vehicle from one place to another, or store it pending inspection, repair or resale, I think the position is clear: they would be in the third residual category. No doubt the on-board computer will start to function when the vehicle is moved; the individuals moving the vehicle might even use the system (e.g. by using the satnav or linking their own phone). However, such use of the system will be purely incidental to the performance of the mandated task.

49. The position of intermediaries who inspect and refurbish a vehicle on behalf of the lessor is potentially different. It will depend on the scope of their instructions. Someone who is instructed simply to carry out an inspection of a vehicle's roadworthiness (akin to an MOT) and to correct any mechanical or cosmetic defects might well avoid any responsibility under data protection law. In most cases though, I would have thought, inspecting and preparing a vehicle for resale will involve checking the on-board computer systems and indeed (since this is what buyers will expect) performing a factory reset so that the system is as good as new when the next owner starts to use the vehicle. If this is what the lessor requires of its inspection/refurbishment contractors, then there would be a good argument that they are "processors": they will deal with personal data in the course of checking and refurbishing the vehicle but, arguably, not just incidentally (as in the case of the IT specialist engaged to fix a software bug) but essentially, since part of the task involves wiping data from the on board system so that the next owner can treat the vehicle as their own.

50. It follows that the lessor should have a controller-processor agreement in place with any company it engages to inspect a vehicle and prepare it for resale (unless that company's role is specifically limited to mechanical/physical/cosmetic matters). It also follows that the inspection/refurbishment company (being a processor) must comply with the instructions in the controller-processor agreement and will also have a free-standing duty, under Art 32, to have in place appropriate technical and organisational measures (i.e. a reasonable care type duty to avoid data breaches).

51. Refurbishers etc whose instructions do not extend to requiring them to inspect on-board systems where personal data might be stored would not, in my view, acquire obligations under data protection law if, incidentally in the course of their duties, they were to come across personal data. If they were to inform the lessor that they had found such data, then the lessor would be under a duty to have it deleted, whether or not they had previously taken reasonable steps to ensure that the system had been wiped.

52. Lastly, I turn to the position of a reseller agent, i.e. the person whom the lessor approaches when, having inspected and refurbished the vehicle, they want to sell it on. The example given in my instructions is an auction house. I shall address that scenario in detail, while noting that it may not be representative of all reseller agents.

53. The distinctive feature of an auction is that the auction house does not acquire legal title to the goods being sold. Rather, the seller and the prospective buyer each enter into contracts with the auction house and, if the prospective buyer's bid is accepted, a contract for sale is then formed between seller and buyer. The process of an auction may involve the auction house taking physical possession of the vehicle and allowing prospective buyers to inspect it, or it may be entirely online. Para 29.4 of the [Company C] Conditions of Entry and Sale provide that "*Unless there is a specific agreement in writing to the contrary between [Company C] and the Seller, [Company C] shall have no obligation to perform a factory reset on a Vehicle's system in case personal data … remains present…".*

54. In my view, in a typical auction scenario (either physical or online) the auction house does not become the controller of the data stored on a vehicle's on-board computer. The auction house simply does not have the essential rights of control over those data during the auction process: they remain with the seller until possession and title passes to the buyer. Neither, in my view, will the auction house be a processor of the data in an ordinary situation: the contract made between seller and auctioneer does not require the auctioneer to do anything with the data that may be stored on a vehicle's systems. If the auctioneer happens to take physical possession of the vehicle, and allow prospective buyers to start the vehicle and check that all its systems are functioning (such that, e.g. some personal data stored on the system are processed), that will be entirely incidental. The auction house will therefore fall into the neither controller/nor processor category acknowledged by the EDPB.

55. Before moving on, I should acknowledge that some auction houses, it appears, do offer additional services whereby they inspect the vehicle and make a representation about the condition of the vehicle: evidence of this comes from cl 4.3.4 of the [Company C] standard conditions (although this refers only to the mechanical condition of a vehicle), as well as information provided by my clients on our initial call. Where this places auction houses, in data protection law terms, will depend heavily on what it is they undertake to do, and on what terms. It seems unlikely to me that an auction house would ever become a controller. It is possible that it may become a processor, acting on behalf of the lessor etc who is selling the vehicle. Nevertheless, for the purposes of this high level overview of responsibilities under data protection law, I would be inclined to assume that auction houses will generally be neither controllers nor processors and that ultimate responsibility for the data stored on a vehicle's system rests with the lessor until such time as the vehicle is sold.

56. Other resellers (second-hand car dealerships and so on), might be analysed differently and it will be necessary to focus on the particular arrangements. I address dealerships below.

Scenario B – Financial services agreements

57. I can take this more briefly because the analysis is essentially the same, in my view, as in Scenario A, with the finance organisation ([Company D] was given to me as an example) standing in the same position as the lessor in Scenario B. In other words, once the finance organisation takes possession of the vehicle (either itself or through an intermediary) it is likely to become the controller of the personal data contained on the vehicle's systems and is likely to be under a duty to remove the data before the vehicle is sold on. The positions of the original user of the vehicle from whom it is repossessed, the intermediaries and the reseller will be the same as in Scenario A.

Scenario C – daily rental organisations

58. This is the familiar scenario where a company (e.g. [Company E]) repeatedly hires the same vehicle to various individuals on short-term hires. The hiring company will retain legal ownership of the vehicle throughout and will be the registered keeper throughout. The driver who hires the vehicle may store personal data, of himself and others, on the vehicle's systems, during the hire period. At least where those data concern third parties (friends and family etc), the driver will be acting as a controller. When the driver hands the vehicle back, that will arguably involve the transfer the personal data stored on the system and, in respect of third party data (friends and family) it will probably involve processing by the driver which falls with the UK GDPR and breaches the data protection principles in Art 5(1). (In other words, the situation is identical to the return of the vehicle by a lessee at the end of a long lease).

59. Upon return of the vehicle, it seems to me, the hiring company will become the controller of any personal data stored on the vehicle's systems, and the only thing that it can lawfully do with those data is delete them. If it re-lets the vehicle without doing so, such that the next hirer can see the previous hirer's personal data, then there will be a strongly arguable case that the hirer has processed the data in contravention of the Art 5(1) principles.

60. For the same reasons given under Scenario A, I do not consider that the hire company can avoid liability by requiring hirers to delete their own data. At best, this would only give rise to a contributory negligence argument which might reduce the amount of compensation payable.

Scenario D - dealerships

61. There are a wide variety of circumstances in which a dealership can find itself in possession of a vehicle which may have personal data stored on it. The position can usually be worked out by analogy with the scenarios already discussed.

62. Take first a very simple example where an individual owner of a vehicle sells it outright to a second-hand car dealer. The seller ceases to be the registered keeper and the dealer acquires all rights of ownership and control until the vehicle is sold on. In my view, in this situation the dealer would be the controller of all personal data stored on the vehicle (whether or not they bothered to inspect it) and duty-bound to erase it.

63. Another situation that I was specifically asked to address is a dealer who is involved in "grounding" a vehicle. As I understand it, this means that they take possession of a leased vehicle at the end of a lease, inspect its condition and then hold the vehicle. At this stage, the vehicle is an asset of the finance company who let the vehicle to the consumer, and the finance company will give the dealer the first opportunity to purchase the vehicle. If the dealer is not interested, the finance company will direct them to dispose of it in another way (e.g. pass it on to another dealership, or to an auction house).

64. In this scenario, unless and until the dealer actually exercises its option to purchase the vehicle, it will not be a controller. It may well be a processor, acting on behalf of the finance company, who would be the controller. That would depend on the extent of the inspections etc that the finance company requires the dealer to undertake (i.e. whether checking for personal data on the system was an integral part of their task, or whether they simply accessed data on the system accidentally or incidentally). If the dealer exercises the option to purchase the vehicle, they would become the controller at that point (again, whether or not they bothered to inspect the vehicle for data).

65. Lastly, dealers will typically provide courtesy cars to customers whose vehicle is being serviced, or offer test drives. In those circumstances, the dealer's position is analogous to that of the daily rental organisation (Scenario C above) and they will become the controller of any data left on the system by the customer when they return the vehicle.

Other questions raised by my instructions

66. The papers provided to me included an Excel document describing seven different "arrangements" that may arise in the automotive trade. I hope that, in addressing the four scenarios above, I have also addressed each of these arrangements.

67. I am also asked to address the three questions raised at the end of [redacted] email of 28 March 2024, and also four questions raised by my instructing solicitors in their email of 23 April 2024 as well as further questions posed as a result of my draft advice. I think the answers to these questions will already be clear from my advice above but, for the sake of completeness, I answer them here, ordering them in a way that should aid understanding:

Who does the GDPR obligations (including security obligations) apply to? ([redacted] Q1)

68. The obligations in Art 5(1) apply to a controller. The principal obligation on a processor is to process data only on the instruction of a controller (Art 29) and they will usually be immune from a claim for compensation if they do so (Art 82(2). However, Art 32 additionally places obligations on both controller and processor to "implement appropriate technical and organisational measures" to ensure the security of processing. Breach of this provision can lead to a compensation claim against both the controller and processor (see, again, Art 82(2)).

69. I have set out above my views on who might be regarded as controller or processor (or neither) in the various scenarios we are considering.

By taking possession of a vehicle containing a previous user's personal data, does the acquiring entity become a data controller and/or joint controller for the purpose of GDPR? ([redacted] Q1)

70. Yes, where that acquiring entity is the lessor/finance house/hire company. Various middlemen along the way may take possession of the vehicle (to convey it to a storage location, to store it, to inspect it etc), but they are likely to be either processors, acting on behalf of the lessor (etc) or to fall outside the scope of data protection law altogether, because their contact with any personal data stored in the vehicle will be purely incidental. A dealership might be a controller, a processor or (unlikely but possible) neither, depending on the precise circumstances (see Scenario D above).

What is the lawful basis to process? Or should the data be deleted? If the data should be deleted, should this be certified to say it has been done properly? ([redacted] Q2)

71. As explained above, where a lessor/finance house/short-term rental agency (re-)takes control of the vehicle, they are likely to become the controller in respect of the personal data stored in the vehicle's on-board computer. There will be a relatively brief window in which they can process those data lawfully under Art 6(1)(b) (contractual necessity), but the only lawful processing will normally be simply deleting those data. If the data are not deleted upon receipt of the vehicle (and in particular if they are transmitted to a new user of the vehicle, by not having been deleted), it is unlikely that there will be any lawful basis for that continued processing.

Does the new possessing entity, when acquiring the vehicle, have the responsibility to delete the personal data, irrespective of who has previously been in possession, used or owned the vehicle? ([redacted] Q3)

72. In my view, yes, where the "new possessing entity" assumes the role of controller (as to which, see above). I do not think that a lessor (etc) who acquires full control of the vehicle and hence the data stored on the on-board computer can shirk this responsibility by requiring the previous user of the vehicle to delete data before return.

Would any of the attached scenarios be classified as a data breach? ([redacted]s Q3)

73. I have explained the meaning of "personal data breach" above. In my view, a lessor (etc) who (re-)gains possession of a vehicle and then passes it on for resale without having wiped the personal data stored in its on-board system may well be acting in breach of Art 5(1)(f) and Art 32 (depending on the "appropriateness" of any measures they have taken to ensure the removal of the data).

74. Similarly, where the user of the vehicle hands it back without having first wiped the personal data, that may count as a data breach insofar as those personal data are those of third parties (friends and family etc) and, again, depending on the appropriateness of any steps they took to avoid this occurring. As explained above, that is unlikely to enable the lessor (etc) to avoid liability for their own failure to remove the data.

Does counsel agree with the ICO's findings? ([redacted] Q4)

75. The ICO's responses have not been consistent, but the final position it takes (email of 26 April 2023) is that "*The controller is the entity that either owns the car or lawfully repossesses it. In the situation you have described the auction house is unlikely to be the controller because they neither own nor have lawfully repossessed the cars*".

76. Insofar as this response is saying that lessors/finance houses/hire companies are the controller when they regain possession of the vehicle, whereas (plain vanilla) auction houses are not, I would agree, for the reasons I have given above. However, neither "ownership" of the car nor "lawful possession" of the car are themselves determinative.

77. The ICO goes on to state that , "*Although the auction house would not be controller for the personal data, we would still expect them to take the necessary steps to ensure it is handled appropriately. In practice, they should ensure the personal data is deleted before the car is sold. They should not knowingly or recklessly enable personal data to be unlawfully shared with another entity*". I am afraid that this is wishful thinking or regulatory overreach by the ICO. An auction house can only be required to delete personal data if it is the controller or processor in respect of those data. Usually, on my analysis, an auction house will be neither. Legal responsibility for deleting data will usually rest with the seller.

Does providing a commercial service constitute "own purposes"? ([redacted] Q1)

78. This question arises from a statement by the ICO prior to its final email. In an email dated 14 April 2023, the ICO stated "*An entity that acquires cars or any other devices for their own purposes which contain accessible personal data, takes on responsibility for that data*".

79. I read the ICO's email as attempting to articulate the test for a controller, which I have addressed above. It is not a replacement for that test and it would be unwise to become fixated upon the ICO's wording. Of course, all the middlemen in the scenarios I have been asked to consider (logistics agents, storage providers, inspectors, refurbishers etc) are providing a commercial service, as are auction houses. However, the fact that someone is providing a commercial service cannot be determinative of the question of controllership. That is determined by the criteria I have set out above. In many instances, these middlemen and auction houses will be, at best, processors acting on behalf of the entity that has (re-)acquired legal possession of the vehicle. Sometimes, their roles will be so incidental that they do not need to be considered under data protection law at all.

What disclosure obligations might a dealership (or other controller or processor) be under? ([redacted] email 13.05.24)

80. All controllers are obliged to provide data subjects with specified information when (or soon after) they begin processing their personal data (UK GDPR Arts 13 & 14). This is usually done in a privacy notice. Since, in my view, the only thing that a lessor, short-term hire company, or dealership (when acting as a controller) can lawfully do when they acquire personal data that has been left on a vehicle is delete it, the article 13 and 14 requirements are perhaps not of great relevance. Technically though, a lessor (etc) should probably include a line in their standard privacy notice stating that, in the event that any personal data are left on a vehicle's systems at the end of a lease etc, it will consider itself the controller in respect of those data and will erase them. A lessor (etc) who thinks they can do anything else with the data would be very bold indeed. I cannot see how they could lawfully sell or share it, for example. If they did think that they could retain and use the data, their privacy notice would have to outline the intended uses and the legal basis.

81. I do not think that lessors (etc) are obliged to tell lessees (etc) that they may be collecting personal data while the lessee uses the vehicle. That would not be the case because, on my analysis, the controller while the vehicle is out on lease/short-term hire etc is the person in charge of the vehicle, and it is they who are deciding what data to store on the on-board system[9]. Controllership arises (or resumes) once the vehicle is handed back to the rental company (etc).

82. More pertinent, perhaps, are the notification requirements in UK GDPR Arts 33 and 34 which arise in the event of a "personal data breach" (defined above). Art 33 requires the processor (if there is one) to notify the controller "without undue delay" after becoming aware of a personal data breach, and requires the controller then to notify the ICO within 72 hours unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Art 34 requires the controller to notify the data subject directly, but only where the breach "is likely to result in a high risk to the rights and freedoms of natural persons".

[9] The position would be different of course, if a short-term hire agency, dealership offering test drives etc, had software installed on the vehicle which reported back in real time, the location of the vehicle, the manner in which it was being driven etc. The hirer (etc) would certainly be the controller of those data.

83. Accordingly, if a lessor (etc) is informed by a reselling agent or the ultimate new owner that personal data have been found on a vehicle, they would have to consider carefully whether they are obliged to inform the ICO and/or the data subject. If the vehicle is still in the possession of a reselling agent at the time, the answer is probably not – the lessor (etc) can just instruct the agent to delete the data before passing the vehicle on. A risk to individuals is unlikely in those circumstances. Likewise if an ultimate new owner contacts a dealer (etc) as a courtesy to say that they found data on the vehicle but immediately deleted it. In other circumstances, (e.g. where it is not clear what the new owner may have done with the data) notification to the ICO may well be in order. If the personal data left on the system is particularly extensive or sensitive (financial information that could be used by fraudsters etc) or there is some other reason to believe that the data subject is particularly vulnerable, then the duty to notify the data subject themselves may arise.

Mechanism for seeking compensation/likely amount

(raised in comments on my draft advice)

84. A claimant who contends that they are entitled to compensation under UK GDPR Art 82 can bring an ordinary civil claim, usually in the County Court.

85. Compensation is not available merely because there has been a breach of the UK GDPR. The claimant must prove that they have suffered "damage" as a result of the breach, i.e. financial loss or non-pecuniary damage such as distress. It is therefore not possible to put forward some sort of "per-vehicle" tariff. Each case will turn on its own facts.

86. A claimant who can only show the bare minimum necessary to bring a claim for compensation (i.e. proof that a third party has accessed the data left on the vehicle, causing them a "well-founded fear" that the data might be misused) will likely obtain only a very modest sum. There are no reported judgments on similar facts but I would not expect an award in such a case to exceed a few hundred pounds. Cases in which the third party does in fact use the data to the detriment of the data subject, e.g. by making unwanted contact with them or using their financial information to make purchases etc, will naturally attract higher awards. Controllers faced with a situation in which the third party has done something entirely unforeseeable and/or criminal with the data might well seek to argue that these eventualities are too remote, or too distinct from their own wrongdoing, to sound against them in damages. Those concepts are familiar in the common law of negligence and an English court will be instinctively attracted to them. There has been no real discussion yet as to whether they can be read across to the compensation regime under UK GDPR Art 82.

87. There was brief discussion on our second call about the possibility of "class actions" (of the sort familiar in the US). These have been effectively ruled out in data protection cases in England and Wales by the Supreme Court's decision in *Lloyd v Google* [2022] AC 1217. Possibly that court will revisit its decision in light of more recent CJEU decisions, but it is certainly not bound to do so, as it would have been while the UK was a member of the EU. Group litigation orders remain a possibility: those are cases where a number of individual claimants bring claims raising similar issues of fact and law, and are managed together, with some costs advantages for the parties.

Regulatory action by the ICO

88. Aggrieved individuals, rather than seeking compensation in the civil courts, may complain to the ICO about alleged breaches of the UK GDPR. The ICO must then investigate the complaint "to the extent appropriate" (UK GDPR Art 77; DPA 2018 s165(1)). It is unlikely, given the enormous demands on the ICO's resources, that it would do very much in response to an individual complaint about a single instance of unlawful processing. The ICO may take more of an interest if it were the case that a particular business is repeatedly infringing data subject rights, or that misunderstanding of the legal position is endemic in the sector as a whole. The ICO has the power to impose very significant fines on a controller or processor (up to either 2% or 4% of annual turnover, depending on the nature of the breach: Art 83).

Conclusion

89. I have summarised my conclusions at the beginning of this advice.

15 May 2024

Aidan Eardley KC
5RB

In the matter of AutoTek21 Ltd

Further Advice

Introduction

1. I provided written advice on 15 May 2024. I am now asked to provide further advice on the following matters:

    1. Does the Advice provided also apply to the EU (i.e. not just for UK GDPR but also in all the other member states)?
    2. Is a company that relies solely on the highly variable and subjective judgement and knowledge of individuals charged with deleting personal data meeting the GDPR standard of "Appropriate technical and organisational measures"?

Application of my advice to processing done in EU member states

2. Data processing of the sort we are concerned with is governed, in the EU, by the GDPR. The GDPR is a piece of directly applicable, directly effective EU legislation. That means that it applies in each Member State without the need for domestic implementing legislation and that it must be applied in the same way in each Member State. Where there is doubt about its meaning and effect, a domestic court can refer a question to the Court of Justice of the European Union (**CJEU**) and the CJEU's answer is binding on the courts of all Member States.

3. The GDPR applied in the UK while the UK remained a member of the EU and continued to apply under transitional provisions until 31 December 2020 (the end of the Brexit implementation period, or IP Completion Day). On **IP Completion Day**, some minor and technical amendments were made to the GDPR, it was renamed the UK GDPR, and it became part of domestic UK law. Some further changes to the status of instruments like the UK GDPR took effect after the end of 2023: see the European Union (Withdrawal) Act 2018 as amended by the Retained EU Law (Revocation and Reform Act) 2023.

4. The legislation around Brexit is highly complex but, in summary, the UK courts are usually required to interpret and apply the UK GDPR in accordance with judgments of the CJEU concerning the GDPR which predate IP Completion Day, unless that would be irreconcilable with some relevant piece of domestic UK legislation, in which case, the UK domestic legislation takes precedence. UK Courts may, but are not required to, take into account CJEU judgments post-dating IP Completion Day. The general principles of EU law are no longer part of UK domestic law, and neither are the provisions of the EU Charter of Fundamental Rights (which includes, at Art 8, a right to protection of personal data). However, this in itself does not permit the UK court to disregard a CJEU decision which was based on those general principles or the Charter.

5. So, the UK courts now have greater latitude to depart from CJEU interpretations of the GDPR when they consider and apply the UK GDPR. Nevertheless, the UK courts have not yet shown any enthusiasm for doing so and it seems unlikely that they will do so: politically, data protection law was not presented in the Brexit campaign as something which the UK ought to be relieved from, and there would be severe practical consequences if the UK were to diverge too far from EU data protection standards, because the EU might then class the UK as a third country which provides inadequate protection for data subjects, resulting in the suspension of the current arrangements which allow the free flow of data between the UK and the EU.

6. For these reasons, my advice (concerning the UK GDPR) is also equally valid in respect of the GDPR itself, and will therefore provide a basis for the legal analysis of data processing done in EU Member States, subject to some important caveats. The important caveats are these:

Application of my advice to processing done in EU member states

7. First, except where an EU measure, such as the GDPR, properly interpreted, says otherwise, the enforcement of EU law rights (including the assessment of damages) is a matter for the domestic law of the member State concerned, so long as that law complies with the EU principles of effectiveness and equivalence. The principle of effectiveness requires a national court to give adequate effect to EU law rights (including, if necessary, by adopting a novel approach to the assessment of damages). National rules should not make it excessively difficult or impossible in practice to exercise EU law rights. The principle of equivalence requires that whatever rules apply to domestic law claims apply equally to EU law claims. The point at which EU law requirements end and domestic law rules about enforcement begin can be difficult to identify in practice.

8. In the case of GDPR Art 82 (the provision that provides a right to compensation in the event of non-compliance with the GDPR) we know the following, either from the plain wording of the provision or from CJEU case law:

   (1) There is a right to be compensated for “material or non-material damage” where that occurs as a result of an infringement of the GDPR: Art 82(1);

   (2) “non-material damage” includes distress and anxiety suffered as a result of the infringement. This extends to a “well-founded” fear that the data may be misused by an unintended recipient, but a purely hypothetical risk (e.g. where no third party actually becomes aware of the data) does not count: BL v MediaMarkSaturn Hagen-Iserlohn GmbH C-687/21, CJEU 25.01.24;

   (3) It is not necessary that the damage reaches a “certain degree of seriousness”: any relevant damage proved to have been caused by an infringement requires compensation: UI v Osterreichische Post AG C-300/21, CJEU 04.05.23

   (4) Usually, it will be the controller who is liable, but it may also be the processor if either (a) the processor has failed to comply with obligations specifically applicable to processors (e.g. the security obligations in Art 32) or (b) the processor has acted outside or contrary to the instructions given by the controller: Art 82(2);

   (5) The controller/processor can avoid liability for damage “if it proves that it is not in any way responsible for the event giving rise to the damage”: Art 82(3);

   (6) The controller/processor is liable for unlawful processing carried out by a person acting under their authority (e.g. an employee): GP v juris GmbH C-741/21, CJEU 11.04.24, [44]-[54];

   (7) Sums payable under Art 82 are compensatory, not punitive: Krankenversicherung Nordrhein C-667/21, 21.12.23;

9. So long as a Member State provides for a compensation scheme that accords with these principles and is, overall, an effective means of compensating data subjects for the damage they have suffered, the particular details of the scheme are a matter for that Member State’s law. That means that there is potential for considerable variation as between Member States. National laws as to what may be taken into account, and how a financial figure should be arrived at, may vary considerably. I am not qualified to advise on these matters of domestic Member State law. Advice should be sought in the relevant Member State.

10. The second caveat is this: in my advice at [25]-[28] I suggested that, where a controller (such as a long-term lessor or short term rental agent) has required their customer to remove their personal data before returning the vehicle, they may be able to reduce any damages they might otherwise be liable to pay by relying on the principle of contributory negligence. That analysis was based on my view that, in the post-Brexit era, the UK statutory provisions on contributory negligence would take precedence over any conflicting provisions and would require a reduction in damages where the driver was at fault to some extent.

11. Since I am now being asked about potential liability in the Member States, it is important to clarify that, arguably, some sort of reduction on the basis of the driver's own failure to delete data may be possible even within the EU law framework. Plainly a controller/processor can only avoid paying compensation entirely if they prove that they were not in any way responsible (Art 82(3)). Arguably however, that does not preclude some sort of reduction to reflect the fault of the data subject, if national law provides for that. So, contributory negligence arguments may be encountered in EU Member States and not just the UK.

12. The third caveat concerns class actions for infringements of data protection law. As I mentioned in my advice at [87], these have been effectively ruled out in the UK as a result of the Supreme Court's decision Lloyd v Google [2022] AC 1217. That was principally because of the narrow way in which the UK legal provisions permitting such actions are drafted. It may be that some EU Member States are more liberal in this regard, such that class actions could be brought by a number of individuals against (e.g.) a car rental operator who failed to delete their personal data. That would increase significantly the legal risk to the relevant businesses. Again, I am not qualified to give advice under the law of particular Member States. Advice should be sought from local lawyers.

13. The fourth caveat concerns GDPR Art 80 which permits Member States to allow not-for-profit representative bodies (e.g. consumer associations like Which?) to raise complaints and seek compensation on behalf of data subjects, either with or without the permission of the data subject. So far, the UK has only permitted this on an opt-in basis (i.e. where the data subject mandates the organisation to pursue a complaint on his behalf): Data Protection Act 2018 s.187. It is possible that some Member States permit representative bodies to bring claims even without instructions from individual data subjects. Such claims are likely to pose much more of a financial threat to controllers than claims where individual data subjects have to opt in, since relatively few data subjects will bother to opt in to a claim which may well be of low value to them as an individual. Once again, advice should be sought from local lawyers to ascertain what sort of actions (if any) it has authorised under Art 80.

Is a company that relies solely on the highly variable and subjective judgement and knowledge of individuals charged with deleting personal data meeting the GDPR standard of "Appropriate technical and organisational measures"?

14. My instructions provide some context for this question. They state:

    There are tens of thousands of different procedures on how to delete the personal data from vehicles, depending on the vehicle make, model, year, trim, system installed (e.g. what infotainment "box" has been installed), and for newer vehicles what firmware version (sometimes software updates change what data is collected, how it is stored, and what needs to be done to delete it).

A situation we often encounter is some companies appoint their employees (e.g. a dealership technician) or their processor (e.g. a third-party inspector or an auto auction) to perform the data deletion, but all those individuals have is their own individual knowledge and experience to decide what sequence of steps to follow for any given vehicle. They receive no tools to guide them on what to do for a specific vehicle, nor to document what steps have been followed.

We know that the very best benchmark we have encountered over the years is that companies that have robust processes (e.g. every vehicle goes through a checklist to ensure workers are prompted to delete personal data, and check this activity off the checklist when they have "completed" the task) but rely on what is in their brain only leave personal data behind in 1/3 of the vehicles. 50-70% is more the norm.

The root cause is, as you can imagine, human error, because nobody on the planet could possibly know what is the exact and correct sequence of steps for any given vehicle. This method also makes it impossible to document what steps were followed for a given vehicle, because any two inspectors may choose a different approach and sequence, again based on their experience and knowledge and judgement.

15. The phrase “appropriate technical or organisational methods” appears in GPDR (and UK GDPR) Art 5(1)(f):

    (1) Personal data shall be:
    […]
    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)

It appears again in Art 32, which supplements Art 5(1)(f):

Article 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    (a) the pseudonymisation and encryption of personal data;
    (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
    […]

16. Whether methods taken to ensure the security of personal data are “appropriate” is a highly fact-sensitive question to be determined in all the circumstances: see e.g. VB v Natsionalna agentsia za prihodite (CJEU, case C-340/21, judgment of 14.12.23), Underwood v Bounty [2022] EWHC 888 at [45]-[48] and Various Claimants v WM Morrisons Supermarkets Plc [2018] 3 WLR 691 at [68]-[70] (these two English cases concern the equivalent provision in the Data Protection Act 1998, the predecessor to the (UK) GDPR). Relevant considerations will include the amount of data, the sensitivity of the data, the potential effects on the data subject if there is a personal data breach or the data are otherwise processed unlawfully, the technical measures available to ensure greater security of processing and the costs of implementing such measures or taking other precautions.

17. Another important feature of the current regime is GDPR/UK GDPR Art 5(2), which provides that “the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”. This places a burden on the controller to show that their security measures were appropriate: VB (above) at [57].

18. In my original advice I was asked to consider a wide range of factual scenarios in which personal data are left on a vehicle’s on board computer system. Given the fact-sensitive nature of the enquiry, it is not possible to give a definitive view as to what a controller must do when they acquire or regain possession of a vehicle. Everything will depend on the particular circumstances. However, I can cautiously offer the following observations.

19. Firstly, where the user of the vehicle (i.e. the long- or short-term lessee) was under a contractual obligation to remove their personal data from the vehicle’s systems, that will be an important factor in reducing the diligence to be expected of the controller to whom the vehicle is returned. However, I would expect a court to be sympathetic to the fact that users may lack the technical expertise (or, in the case of short-term rentals, the time) to effectively cleanse the system, so this consideration may have a fairly limited effect in reducing the burden on the controller unless clear and simple instructions for deletion are given.

20. Secondly, an important factor will be the ease with which any personal data stored on the vehicle could be accessed by a future user. Data that is buried deep within a computer system and which is unlikely to be discovered through casual use is unlikely to pose much of a threat and, if an ad hoc manual inspection of the system fails to pick up every last piece of such data, that is unlikely to put a controller in breach of art 5(1)(f). By contrast, if the personal data is stored in a way which means that the next user of a car will readily come across it during normal use of the vehicle, a controller may well need a system in place that is aimed at removing such data.

21. Thirdly, the quantity of data stored on the vehicle’s system, its sensitivity, and the potential for it to cause real harm to the data subject if it is accessed by a subsequent user, are all factors that are relevant to determining what is required by way of an appropriate measure. It might be thought that these risk factors are lower in the case of short term rentals and higher where the user has had the vehicle for a considerable amount of time. Data (even if it counts in law as personal data) about where or how a vehicle has been driven in the past is unlikely to pose much of a risk. Data such as home addresses, telephone numbers, and app logins where a subsequent user of the vehicle might be able to use the login to access inappropriate content or to charge purchases to the credit card of the previous user are much more sensitive and a controller who does not have a system in place that will reliably remove such data may be at significant risk of an adverse finding.

22. Fourthly, a controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in (UK) GDPR Art 5(2) to demonstrate compliance. A controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed.

23. Beyond these general observations, I am not able to provide advice of any real value given the highly fact-sensitive nature of the exercise. If my clients come across specific scenarios in which the appropriateness of a controller's measures is in issue, I may be able to give more focussed advice.

24. Lastly, there is this point. In my original advice, I identified arguments that (1) an entity that acquires or regains possession of a vehicle becomes a controller of the personal data contained on the vehicle's on-board computer; (2) that entity has no legal basis for continuing to store (and hence, process) that data once the brief initial period for deleting it has expired; (3) insofar as the onward sale or re-rental of the vehicle might be said to involve the disclosure (and hence processing) of the personal data still stored on its systems, that processing would also have no legal basis; and (4) a failure to delete unnecessary data would additionally be a breach of the data minimisation principle in Art 5(1)(c). See, in particular, my original advice at [39]-[40]. Liability for breaches of Art 5(1)(a) (which requires a legal basis for processing) and Art 5(1)(c) (requiring data minimisation), is strict. It does not depend on proof that a controller has or has not employed appropriate measures to avoid a breach. Accordingly, so long as a data subject can prove that the harm they have suffered through disclosure of their data to third parties is the result of the controller's unlawful storage, unlawful failure to minimise and/or unlawful disclosure of that data then they will be entitled to compensation, regardless of whether the controller took "appropriate measures" as required by Art 5(1)(f) and Art 32.

25. I anticipate that cases founded on alleged breaches of Arts 5(1)(a) and 5(1)(c) will be hotly contested (at what point does the contractual necessity legal basis under art 6(1)(b) cease to operate; does physically handing over a vehicle with an on-board computer system amount to disclosure, and hence processing, of the personal data stored on the system; was the unlawful storage of the data and/or the unlawful failure to minimise it truly causative of the harm to the data subject that occurred? etc). Controllers are likely to argue that such cases should really be analysed under Art 5(1)(f) and that their security measures were appropriate. Nevertheless, until a court says otherwise, it seems to me that there is a real risk for vehicle lessors etc that they may be held liable for damaging disclosures of personal data in breach of (UK) GDPR Art 5(1)(a) and/or (c) whether or not they may have complied with Art 5(1)(f) and Art 32.

Conclusion

26. In answer to the first question, my original advice applies equally to the position of lessors (etc) in the EU, subject to the caveats that I have set out above.

27. In answer to the second question, I cannot say definitively whether reliance upon the knowledge and judgement of individuals tasked to remove personal data from vehicles will or will not satisfy the requirement for "appropriate technical and organisational measures" because the issue is too fact-sensitive. However, I have identified above some material considerations. I have also re-iterated some arguments to the effect that a person who takes possession of a vehicle containing personal data may find themselves liable for processing those data without a proper legal basis and/or in breach of the data minimisation principle (GDPR Arts 5(1)(a) &(c)) whether or not they could also be criticised for failing to take appropriate technical/organisational measures to ensure the security of those data (GDPR Art 5(1)(f) & Art 32).

2 September 2024

Aidan Eardley KC
5RB

In-Vehicle Data Deletion Process Guidance for Processors and Controllers

Background: GDPR compliance requires that the personal data of individual users of vehicles (“Data Subjects”) stored in the non-volatile memory of the vehicle is deleted by the Controller (or a Processor of their choosing) at every vehicle handoff, e.g. at the return of a lease, at remarketing, at the end of a rental or carsharing, after a total loss accident, etc. GDPR specifies some minimum standard on how this operation ought to be performed. In addition, businesses may want to add requirements that, although fall outside of GDPR minimum requirements, are beneficial for the process to be economically viable.

Objective: This document provides guidelines for businesses to implement and continuously maintain a data deletion process to ensure a robust and compliant removal of personal data from the electronic systems of a vehicle before it changes hands. The process should adhere to the following "Appropriate technical and organisational measures":

1. Technical Means of Data Deletion:

    1.1 Data deletion can be achieved through either (a) the physical destruction of the medium, (b) a deletion that can resist forensic techniques in a lab, or (c) a data clearing. For vehicles, (a) is economically unfeasible and should be reserved for extreme cases, (b) is technologically unavailable.

    1.2 Consequently, data deletion in vehicles should be achieved through logical operations, using a combination of factory resets and overwriting (i.e., "data clearing" and "sanitisation" according to the 800-88 rev 1 standard and "media sanitisation" according to ISO/IEC 27040).

    1.3 There are tens of thousands of variations in the process to perform a data clearing, depending on the vehicle make, model, year, trim, and infotainment firmware version. The specifics of what data can be deleted and how it can be deleted vary accordingly.

    1.4 As a standard, the process must delete all personal data stored in the vehicle infotainment system and, if equipped, OEM garage door/gate openers – as allowed by manufacturer-designed systems and methods (i.e. no hacking).

2. Objective and Repeatable Process:

    2.1 The process must be objective and repeatable, regardless of the individual or organisation performing the data deletion.

    2.2 To avoid significant negative outcomes (e.g. GDPR non-compliance), the process cannot solely rely on subjective judgement or experience of individuals. The King’s Counsel opinion referenced in this whitepaper clarified that “best endeavours” approaches do not meet the standards set by the law. Controllers should establish a proper in-vehicle personal data deletion policy for the vehicles in their control, i.e. with demonstrable, appropriate technical and organisational measures. A Controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in (UK) GDPR Art 5(2) to demonstrate compliance. A Controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed.

2.3 It follows that the most robust and compliant process requires to offer operators a sequence of logical and orderly steps for personal data deletion on a VRM (Vehicle Registration Mark) or VIN (Vehicle Identification Number)-specific basis. Such a process creates safeguards for consistent and repeatable execution, since any two operators would follow identical documented steps to delete personal data from the same vehicle.

3. Reliability, Robustness, and Resilience:

3.1 The solution must be able to demonstrate reliability, robustness, and resilience.

3.2 Reliability, able to perform its intended function adequately for a specified period of time, or operate without failure.

3.3 Robustness, the capability to cope with errors during operation, cope with erroneous data input and exceptional circumstances.

3.4 Resilience, the ability to adapt and respond to changing inventory, and exceptional circumstances, to maintain essential operational capabilities.

4. Detailed Record Keeping:

4.1 GDPR compliance requires records to be produced and retained to prove that the data deletion has been performed.

4.2 At minimum, records must document what vehicle was processed, when, what systems were cleared, the attestation of the operator that the process to clear the data for that vehicle was followed as prescribed, and the outcome of the operation.

4.3 Should any exceptional circumstances prevent the process from being followed (e.g., non-operational infotainment system, operator safety concerns), those reasonable exceptions must be documented and reported as well.

4.4 It is advisable that the solution record the location and operator (or work-team) performing the deletion for accountability and chain-of-custody considerations.

5. Data Minimisation and Transparency for Data Subjects:

5.1 GDPR requires Controllers and Processors to minimise the processing of personal data. Consequently, the solution should avoid collecting any personal data from the vehicle or documenting any content or setting that may be reconducted to an individual. The only identifier that should be collected is the vehicle identifier, which is necessary to prove all vehicles exchanging hands have been properly processed for data deletion.

5.2 GDPR also requires transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing.

5.3 Consequently, data subjects (i.e., individual vehicle users) must be able to access and independently verify records confirming if and when a Controller (or their Processors of choice) performed a personal data deletion from a specific vehicle.

Additional business considerations: While not strictly required for GDPR compliance, the following best practices should be considered by Controllers and Processors:

- Processors should have a standard addendum detailing how they would perform a data deletion service for the Controllers. That addendum must be presented and a data deletion service offered as soon as reasonably practical to all Controllers. Should Controllers elect to not perform a data deletion via the Processor will hold such Processor harmless.

- Whenever Controllers hire a Processor to perform the vehicle data deletion, the process and records must meet the dual purpose of proving the compliance of Controllers and the operational and accounting needs of Processors. By means of example, best-in-class solutions offer inventory management and operational reporting capabilities, in addition to the ability to generate, download, and share records.
- Records should be interoperable, so that a Controller hiring multiple Processors (e.g. for different parts of their portfolio or different geographies) can obtain uniform compliance logs.
- It should be easy for Processors and Controllers to set-up the service.
- The process should require a low skill level and little training. Average processing time per vehicle should be short to maximise efficiency and minimise operating cost. Solution should not require significant/any Capex, including avoiding proprietary hardware and dongles.

By adhering to this guidance, businesses can ensure reliability, robustness, resilience and a compliant data deletion process that protects personal data and meets regulatory requirements.

SAMPLE LETTERS SENT TO AUTOMOTIVE BUSINESSES

Exhibit 1: Sample Letter Sent to Associations

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. Following the release of the new legal opinion of a King's Counsel, I want to personally reach out and encourage your association to raise awareness on this matter of GDPR compliance within your members. I often speak at conferences and at associations like yours, and I remain available to you or I am happy to connect you with resources to reduce the risk exposure of your members - a key role your association has taken in the past.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – applies to [redacted] members, of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to businesses like those of your members in regard to the personal data captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information, and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. A company becomes the Controller under GDPR of the personal data of prior drivers and passengers stored in vehicles every time they receive them into their possession (i.e.. at lease end, rental end, loan end, on trade-in, at repossession etc.).
2. As Controllers, they are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield them from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. The company (or their Processor, if they use a third party to carry out the data deletion from the vehicles in their possession) must have "appropriate technical and organisational measures" in place "to ensure demonstratable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 2: Sample Letter Sent to Dealerships and Bodyshop and Repairers

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – apply to dealerships and bodyshop and repairers, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal data captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. Your company becomes the Controller under GDPR of the personal data of prior drivers and passengers stored in vehicles every time you receive them into your possession (e.g. lease returns; trade-ins; dealer-purchased vehicles (wholesale/retail), courtesy or loan cars etc.)
2. As Controller, you are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company (or your Processor, if you use a third party to carry out the data deletion from the vehicles in your possession) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 3: Sample Letter Sent to Motor Finance, Fleet Management, and Leasing Companies

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – apply to Motor Finance, Fleet Management and Leasing companies, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal information captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. Your company becomes the Controller under GDPR of the personal information of prior drivers and passengers stored in vehicles every time you receive them into your possession or control i.e. direct returns or indirect returns (e.g. via collection/inspection agent, PCP/PCH returns; repossessions and voluntary terminations, when purchasing or disposing of vehicles directly (wholesale and retail sales) etc).
2. As Controller, you are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company (or your processor, if you use a third party to carry out the data deletion from the vehicles in your possession) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 4: Sample Letter Sent to Motor Insurance Companies

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – apply to Motor Insurance companies, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal information captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. Your company becomes the Controller under GDPR of the personal information of prior drivers and passengers stored in vehicles every time you receive them into your possession or control. You are responsible for deleting, or tasking your 3rd party agents to delete, personal data in vehicles when you, or your agent or representative, gains possession or control of a vehicle e.g. PCP/PCH returns; repossessions and voluntary terminations, written-off or salvaged to be sold for parts, etc.
2. As Controller, you are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company (or your Processor, if you use a third party to carry out the data deletion from the vehicles in your possession) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 5: Sample Letter Sent to Car Rental, Carsharing and Shared Fleet Companies

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – apply to car rental, carshare and shared fleet companies, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal information captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. Your company becomes the Controller under GDPR of the personal information of prior drivers and passengers stored in vehicles between different hirers or users etc. (i.e. at the end of each short-term let or use).
2. As Controller, you are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company (or your Processor, if you use a third party to carry out the data deletion from the vehicles in your possession) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 6: Sample Letter Sent to OEM Manufacturers

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion, about how GDPR – both UK and EU versions – apply to Automotive Manufacturers, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal information captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification.

Here are just a few of my key takeaways from the opinion:

1. Your company becomes the Controller under GDPR of the personal information of prior drivers and passengers stored in vehicles every time you receive them into your control or possession, between different users, including: Demonstration Fleets; Corporate Fleets; Employee Fleets; Press Fleets and Event Fleets, etc.
2. As Controller, you are mandated to delete this data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers or users. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company (or your Processor, if you use a third party to carry out the data deletion from the vehicles in your possession) must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

Exhibit 7: Sample Letter Sent to Motor Auctions; Inspection, Refurbishment and Storage Companies; and Recovery and Repossession Companies

[redacted]

09 Sept 2024

Dear [redacted]

My name is Andrea Amico, founder of Privacy4Cars and a trusted vehicle privacy expert. I often speak with the media on vehicle privacy-related matters and am always looking for businesses in automotive that are doing the right thing to showcase. Following the release of the new legal opinion from a King's Counsel, I want to personally reach out to see if you are meeting those GDPR compliance criteria - and if not, offer to connect you with resources from my network to help you do so.

My team and I recently received the legal opinion about how GDPR – both UK and EU versions – apply to Motor Auctions; Inspection, Refurbishment and Storage Companies; and Recovery and Repossession Companies, including [redacted], of Aidan Eardley, King's Counsel: a barrister at the London BAR with expertise in data protection. This opinion addresses the legal compliance obligations that apply to companies like yours in regard to the personal information captured and stored in vehicles (locations visited, phone records, and much more). As a courtesy, we've provided the full opinion for you at https://privacy4cars.com/gdpr. We highly recommend your legal and compliance teams review this information and reach out to me for any questions or clarification

Here are just a few of my key takeaways from the opinion:

1. Acting on behalf of a Controller, your company becomes the Processor under GDPR of the personal information of prior drivers and passengers stored in vehicles when you receive them into your possession from a lessor (or other type of consignor) and are required to inspect and prepare for resale. Your company should have a written data processing agreement in place with your client outlining responsibilities of Controllers versus Processors.
2. As Processor, acting on behalf of a Controller, you are required to delete this personal data; not doing so is considered a "Personal Data Breach" and can result in substantial business risk, including fines, civil penalties, reputation harm, loss of insurance coverage, etc., and triggers reporting obligations to the relevant Data Protection Authority and data subject.
3. Controllers cannot contractually assign this legal responsibility to their customers. Requesting that individuals/data subjects delete their own data is inconsistent with GDPR and does not shield you from responsibilities nor risks.
4. "Best endeavours" are not sufficient for compliance. Your company must have "appropriate technical and organisational measures" in place "to ensure demonstrable and measurable compliance."

If your members have a repeatable, measurable, documented process in place to delete consumer data from vehicles that adheres to the requirements of GDPR, and this as outlined in this opinion, I'd like to hear from you to celebrate and highlight their care for consumer privacy. If they don't, I'd also like to hear from them to connect them to a few resources that can help.

Your sincerely,

Andrea Amico

Andrea Amico, Founder & CEO, Privacy4Cars

APPENDIX: SAMPLE POLICIES, DISCLOSURE STATEMENTS AND AGREEMENTS

Appendix 1: Sample Controller Policy and Disclosure Language Covering Personal Data Captured By Vehicles

Many vehicles today can collect and even transmit (through wired or wireless connections) information linked to the vehicle, its users, its occupants, and their personal devices (“Vehicle Data”). Vehicle Data can be collected by the vehicle through its sensors, during use or when the users or occupants connect a personal device such as a smartphone. While some of the Vehicle Data will consist of vehicle diagnostics and operational information that is unlikely to identify or profile individuals, much of this Vehicle Data is personal and linked to user or occupant of the vehicle. This may include but is not limited to contacts, 3rd party apps, IDs/biometrics, call logs, text messages, navigation history, home address, garage codes, health and credit data, smart access, users' profiles, and passwords. The Vehicle Data is locally stored, can be potentially be accessed by third parties (i.e. other than the Data Subject who generated the data) and the data linked to a user or occupant (“in-vehicle personal data”) falls under the definition of Personal Data under the General Data Protection Regulation (GDPR).

Accordingly, it is the policy of this company to reasonably attempt to delete in-vehicle personal data from all vehicles in which we, or our associates, take possession, unless:

A. The vehicle is not equipped with technologies capable of storing personal data that can be easily accessed by unauthorised third parties (e.g. navigation history, paired phones, etc.)

B. The vehicle is destined to be returned to the data subject after a brief holding period (e.g. in the case of vehicle maintenance or repair)

C. There are documentable exceptions that reasonably prevent us from attempting to clear and delete the in-vehicle personal data (e.g., we are not provided with a set of keys, the system is malfunctioning or destroyed, for the safety of our personnel, etc.)

Deletion will be done by attempting to systematically delete or make unavailable the in-vehicle personal data using robust industry practices with repeatable, objective, and documented procedures at or about the time we take possession of the vehicle and in any case prior to handing it off to another party. Specifically, in-vehicle personal data deletion will be done and documented as follows unless otherwise required to perform service, recall, or warranty work or to comply with applicable law.

Assessment of applicability of in-vehicle personal data deletion processing:

For every vehicle that comes into our, or an associates, possession we will make a determination to whether a vehicle should be processed for in-vehicle personal data deletion. We will do so in one of three possible ways [check applicable method or delete non applicable methods]:

1. We will conservatively assume that all vehicles should be processed and have the in-vehicle personal data reasonably attempted to be deleted. This is our default method because it minimises risk to customers or data subjects.

2. We will use a VRM or VIN decoder to determine which vehicles are most likely to contain systems that can store in-vehicle personal data and to determine the sequence of steps to be followed for in-vehicle personal data deletion for that specific vehicle. Our personnel will document and skip the vehicles that do not appear to contain such systems.
3. Data subjects have the right to access documentation and records proving that the in-vehicle personal data deletion process was followed in line with this policy. Those records will include a unique identifier for the vehicle (i.e., the VIN or the VRM if uniquely associated with a VIN) but to be privacy-preserving should not include any details about the in-vehicle personal data that was deleted. We will make available summaries of those records.

Recommended in-vehicle personal data deletion management:

The Data Protection Officer (“DPO”), i.e. the individual in our organisation tasked with monitoring GDPR compliance (Art. 25) will be responsible for implementing and monitoring the in-vehicle personal data deletion process.

1. In-vehicle personal data deletion responsibilities will be delegated to one or more designated employees or third-party associates. The employees charged with the in-vehicle personal data deletion task will follow an objective, repeatable, and measurable process and produce electronic records documenting the date of the deletion, the systems processed for data clearing, and the completion of the process (“deletion records”). If the in-vehicle personal data cannot be deleted for technical or systems issues involving the vehicle, the employee will produce an electronic record indicating the date of attempted deletion and the reasons why the in-vehicle personal data deletion could not be completed (“exception records”). The employee must sign and date the deletion records or exception records (electronically or with wet ink) and file them as directed by the DPO or their authorised deputy. The DPO must have technical, administrative, and physical systems in place to monitor the data deletion activity, verify the completeness and accuracy of the records, and audit the quality of the work of the designated employees or third party associates.
2. We acknowledge that we may take temporary custody of vehicles with vehicle data for purposes of servicing, recall, or warranty work. With respect to nonpublic personal data, it is the policy of this company not to access, disclose, or use the vehicle data in such vehicles at any time except as and to the extent necessary to perform the service, recall, or warranty work. The following language will be added to all servicing and warranty repair orders:

   > “Customer acknowledges that the subject vehicle may contain GDPR-regulated personal data concerning their customers or its use of the vehicle in an embedded form. This data may be acquired natively by the vehicle or by synchronising with the consumers’ devices such as smartphones.
   >
   > Company takes no interest in the in-vehicle personal data, and it is the policy of this company and its authorised processors not to access, use, or disclose the in-vehicle personal data to any person, except as necessary to perform the services requested by the vehicle owner or as required by the OEM. Access by the vehicle’s OEM or other parties may have been previously authorised by the customer. Except as necessary to perform the service, recall, or warranty work or comply with provisions of law, the provider will take no action with respect to the in-vehicle personal data unless the vehicle owner provides a written request to delete any data.”
3. The DPO or its designees will make reports concerning compliance with these procedures along with recommending any changes. Such reports will be made not less often than annually in connection with the provider’s GDPR compliance review.

Appendix 2: Sample Disclosure Statement For Processors of In-Vehicle Personal Data To Notify Customers That Are Controllers Of Same

To: [Controller entity name (customer or Processor)]

From: [Processor entity name (third-party provider of Controller)]

IMPORTANT NOTICE CONCERNING SAFEGUARDING IN-VEHICLE PERSONAL DATA IN ACCORDANCE WITH GDPR

You have delivered to our possession certain vehicles for inspection that are destined to be handed off to a new vehicle owner/user.

Under the General Data Protection Regulation (GDPR), you are responsible for safeguarding the personal data of data subjects who have previously owned or used the vehicle, before it changes hands. This includes all personal data that is physically stored on the vehicle systems (in-vehicle personal data) and could be accessed by unauthorised third parties, including future vehicle owners and users unless properly disposed of. By means of example, in-vehicle personal data includes stored addresses, location history, data from phones connected to the infotainment system, garage door codes etc. To understand your obligations as a Controller, we encourage you to review the legal opinion of Aidan Eardley, King's Counsel, and additional materials available at https://privacy4cars.com/gdpr

As a Processor, it is the policy of this company that we will delete in-vehicle personal data in line with GDPR requirements from all vehicles you, the Controller, physically deliver to us directly or through a nominate transport agent and that you/the original owner does not redeem and for which you provide us with reasonably sufficient time to process (two business days). Our company will make commercially reasonable attempts to systematically delete or make unavailable the vehicle's in-vehicle personal data using robust industry practices with repeatable, objective, and documented procedures at or about the time we take possession of the vehicle and in any case prior to handing it off to another party. You agree to reimburse our costs of undertaking to do as outlined below, which costs will be included in a succeeding bill for services or added to the bill for processing of the vehicle.

We will use a VIN/VRM decoder to determine which vehicles are most likely to contain systems that can store in-vehicle personal data and to determine the sequence of steps to be followed for the in-vehicle personal data deletion for that specific vehicle. Our personnel will document and skip the vehicles that do not appear to contain such systems. Our personnel will also document exceptions that reasonably prevent us from attempting to clear and delete the in-vehicle personal data (e.g., we are not provided with a set of keys, the battery is flat, the system is malfunctioning or destroyed, for the safety of our personnel, etc.). We will hold each other harmless for reasonable or infrequent errors and omissions that may result in consumer personal data being left in vehicles.

Since data subjects have the right to access documentation and records proving that the in-vehicle personal data deletion process was followed in line with GDPR and this policy, we are making those records available to you upon request. Those records will include a unique identifier for the vehicle (i.e., the VIN or the VRM if uniquely associated with a VIN) but to be privacy-preserving should not include any details about the in-vehicle data that was deleted. We will publish summaries of those records.

Your delivery of the vehicles to our possession and continuing to leave the vehicles with us constitute your agreement to these terms.

Appendix 3: Sample Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between:

[Company Customer] a company incorporated in England and Wales under No. [xxx] whose registered office is at [address], with designated email address [address] (the "**Company**") and

[Company Supplier] a company incorporated in England and Wales under No. [xxx] whose registered office is at [address] , with designated email address [address] (the "**Data Processor**")

(together as the "**Parties**") **WHEREAS**

a) The Company acts as a Data Controller.
b) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
c) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Data Protection Act (DPA) 2018 and General Data Protection Regulation (GDPR).
d) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:

1.1.1 **"Agreement"** means this Data Processing Agreement and all Schedules;

1.1.2 **"Company Personal Data"** means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 **"Contracted Processor"** means a Sub-processor;

1.1.4 **"Data Protection Laws"** means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 **"Data Subject"** means a person or persons that has provided personal data to the Customer directly or indirectly through the use of its products, services or solutions.

1.1.6 **"UK Data Protection Laws"** means Data Protection Act (DPA) 2018, as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 **"GDPR"** means UK General Data Protection Regulation;

1.1.8 **"Data Transfer"** means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 **"Services"** means the products, services or solutions the Company provides.

1.1.10 **"Sub-processor"** means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, **"Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws (Articles 5(1) and 5(2) of the GDPR) in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

2.2.1 Data processing comprises of the act of destruction of Company Personal Data (i.e., "media sanitisation" according to ISO/IEC 27040), unless required or authorised by the Company.

2.2.2 Data processing must delete all personal data stored using a sequence of logical and orderly steps for consistent and repeatable execution, multiple processing personnel should follow identical documented steps to delete personal data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless required or authorised by the Company.

6. Processing of Company Personal Data

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

10.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

11. Data Transfer

11.1 The Processor may not transfer or authorise the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 **Confidentiality**. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of England and Wales.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England and Wales, subject to possible appeal to Court of Appeal

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Company

Signature

_____

Name:

_____

Title:

_____

Date Signed:

_____

Data Processor

Signature

_____

Name:

_____

Title:

_____

Date Signed:

_____

Schedule 1 - Processing Activities

This Schedule 1 includes certain details of the Processing of Personal Data as required by Article 28(3) UK GDPR. The subject matter and duration of the Processing of the Personal Data are set out in the Agreement and this DPA.

The nature and purpose of the Processing of Personal Data

The Data Processor will Process Personal Data as necessary to provide the Services pursuant to the Agreement, and as further instructed by the Company in its use of the Services.

The types of Personal Data to be Processed

The Company may submit Personal Data to the Data Processor, the extent of which, is determined and controlled by the Company in its sole discretion, and which may include, but is not limited to the following types of Personal Data:

- Deletion of Personal data in the Infotainment system and/or onboard computer

The categories of Data Subject to whom the Personal Data relates

The Company may submit Personal Data from Data Subjects to the Data Processor, the extent of which is determined and controlled by the Company in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Data Subjects, vehicle drivers, users and passengers, including their employees

Schedule 2 - Technical and Organisational Measures

The **Data Processor** will conduct the activities covered by this DPA in compliance with its Information Security Policy, available from the Data Protection Officer or another person responsible for data protection compliance, and relevant data protection policies and guidance, available from the Data Protection Officer or another person responsible for data protection compliance.

Schedule 3 - Sub-Processors

The Customer agrees that the Data Processor may sub-contract certain obligations under this DPA to the following Sub-processors:

Name of Sub-processor: [Name]

Contact details:

Email address: _____

Telephone number: _____

Subcontracted Activities:

_____

Using Privacy4Cars to Delete Personal Data from Vehicles: Your Solution to Meet GDPR Data Deletion Requirements

Automotive Businesses GDPR Legal Obligations:

Automotive businesses must delete the personal data of previous drivers and passengers before a vehicle changes hands (e.g. trade-in, lease return, loan return, rental return etc.) under GDPR.

> *"A Controller who relies only on the subjective experience and knowledge of individual employees may struggle to meet the requirement in [UK & EU] GDPR Art 5(2) to demonstrate compliance. A Controller who uses a documented procedure for cleansing an on-board computer system and/or a software product designed to remove problematic data will be much better placed."*
>
> *- Aidan Eardley, King's Counsel of the London BAR*

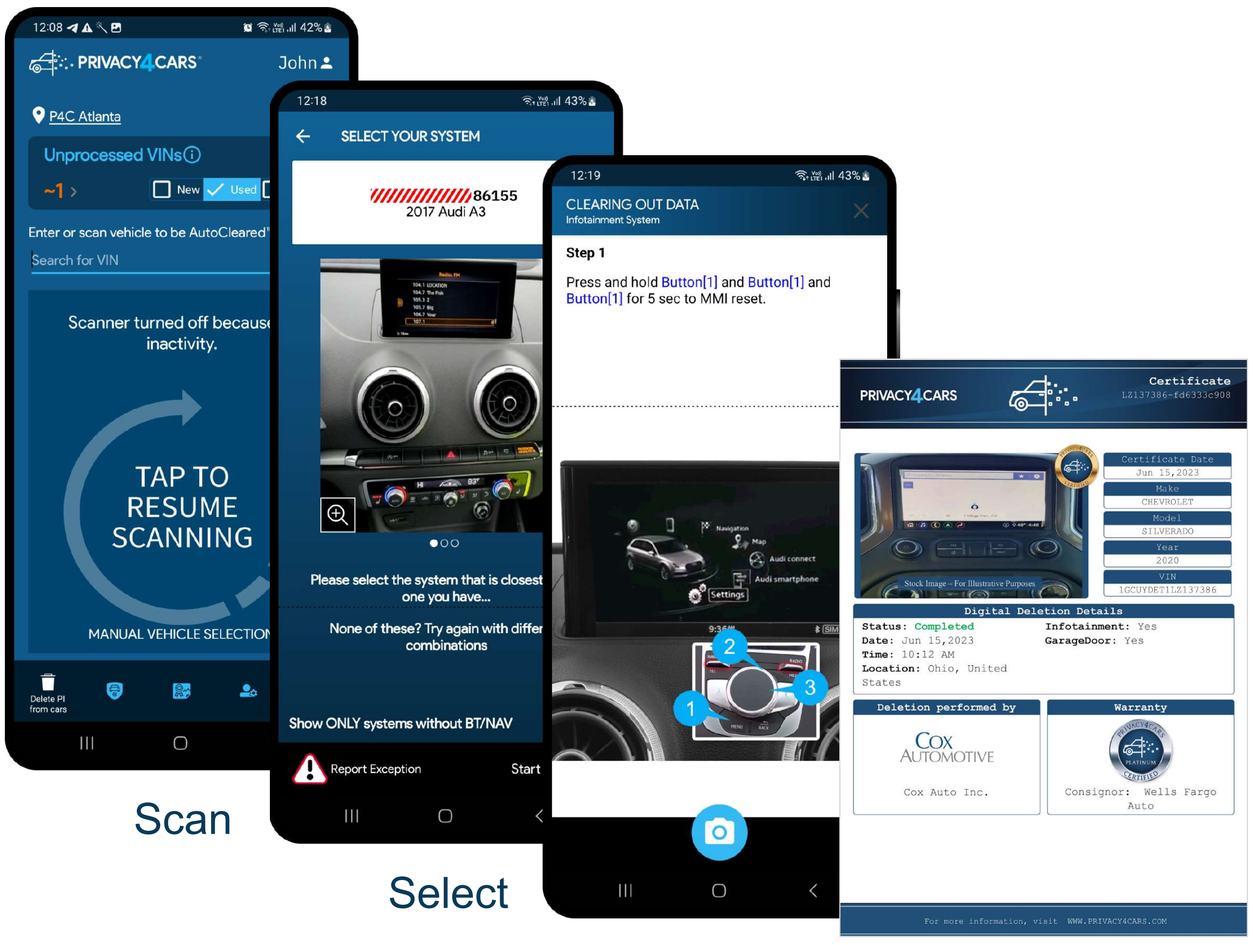
How Privacy4Cars Helps Your Business Meet GDPR Requirements:

Privacy4Cars' AutoCleared™ delivers fast, reliable, repeatable and auditable results. The quick and easy to use solution enables businesses to seamlessly integrate GDPR compliance into their existing processes. Leading automotive businesses, such as: dealerships, leasing and fleet management, motor finance, motor insurance, car rental/car sharing companies, manufacturers and more, choose Privacy4Cars to meet compliance requirements.

Privacy4Cars enables automotive service providers to generate new revenue by offering data deletion services to their clients. With Privacy4Cars, service providers demonstrate they do not rely on the subjective knowledge of their personnel, but rather have the appropriate technical and organisational methods that their clients require for GDPR compliance.

Industry leaders have used Privacy4Cars to clear personal data from over 2 million vehicles.

Privacy4Cars can get you started in as little as one business day.



Scan Select Follow Certify

A Simple, Certifiable & Compliant Process:

Scan the VIN/VRM and the solution will identify the vehicle and the step-by-step deletion instructions that apply to that specific vehicle.

Select the exact infotainment system.

Follow the steps to drive consistent, reliable, efficient deletions; subjective knowledge is unreliable & non-compliant.

Certify and build complete, accurate, measurable records of compliance. Certificates are sharable (APIs available).

Schedule an Appointment Today!

Privacy4Cars, the world's leading authority on vehicle privacy & data security. Learn more:
Call: +44 203 488 4642 or email: gdpr@privacy4cars.com