Data Privacy in the Context of APDS

Guidelines for protection of personal data

Release 1.0

May 2025

© Copyright – Alliance for Parking Data Standards Limited and European Parking Association

Document Version Control

Date	Release	Status
May 2025	Release 1.0	Published for General Review and Comment

Contributors

Bernd Reul	Principal Author
Keith Williams	Principal Author
Markus Schneider	Editor
Stefan Sadleder	Editor
Ties de Groot	Editor
Rob Rome	Editor
Tom Antonissen	Editor

© APDS 2025

© APDS 2025

Contents

© APDS 2025

1. Introduction

Data privacy is a concept that organisations of all sizes currently manage in modern business. Each organisation will have different degrees of complexity, according to their relationships with their suppliers, customers (those they provide services to) and, of course, the public. Local, National or Regional legislation will have a bearing on the contractual agreements that are required.

There are a number of privacy laws around the world, each of which attempts to address the issues in either their own geographic or data domains. Examples include HIPAA (relating to medical information), CCPA (which focusses on the rights of consumers in relation to businesses) and GDPR (establishing the rights of individuals in the European Union and EEA countries (i.e. Iceland, Liechtenstein, and Norway). GDPR is arguably the most far reaching of these, so to some extent, the rest of this document uses GDPR as its reference. It is to be noted that, although the GDPR is a regulation directly applicable in all the EU Member States with the aim to ensure harmonization of the data protection rules, the GDPR also gives a certain margin of manoeuvre for the Member States to further specify some elements of the GDPR. Therefore, each EU Member State has adopted its own national data protection legislation that implements and complements the GDPR. This may lead sometimes to national specificities which have to be taken in consideration to ensure compliance with the applicable data protection legislation.

APDS provides an opportunity to bring some clarifications on the interpretation of the main rules and principles under the GDPR. If data can be standardised to everyone's benefit, then so can data privacy arrangements. It should be noted that in this document, "**APDS**" is used to refer to the **APDS organisation** and "**APDS specifications"** is used to refer to the technical specifications published by the APDS organisation.

2. Scope

Following on from its work on parking data specifications and APIs, APDS has identified a need to develop a set of industry guidelines with recommendations as to how data protection principles should be applied to parking. The intention is that these guidelines will be used to help achieve compliance with the main requirements stemming from the GDPR.

The guidelines are intended to provide an overview of the key issues.

THEY ARE NOT A DEFINITIVE STATEMENT OF LAW.

The guidelines are intended only to provide context for anyone intending to share such data, enabling them to then use appropriate resources to determine exactly the steps they should take to develop good practice in data management and remain compliant within their jurisdiction.

Care should be taken when determining the relevant jurisdiction. For example, in some situations the GDPR can apply to - companies based in the EU but operating in the US and to companies based in the US but operating in the EU -.

The intention is to create a unified view, to the extent possible, on:

- Roles and the associated responsibilities (data Processor/Controller, etc)
- The types of data that are considered personal data in the sense of the GDPR.
- And to create and publish guidance on:
- How the APDS specifications can support compliant handling of personal data when that data is being shared?
- GDPR-compliant handling of personal data within intra-industry agreements

3. What is Personal Data?

It is worthwhile noting the breadth of information considered to be personal data. Some, such as name, address and telephone number are not controversial. Similarly, bank account and credit card details are self-evident. Less obvious examples might include a vehicle registration number, IP address or location data.

GDPR has possibly the most comprehensive definitions of what constitutes personal data[1]. The UK Information Commissioner's Office (ICO) provides clear guidance on interpreting GDPR and identifying whether data is personal or not. Whilst this guidance is generic it provides a good starting point.

Six points from the guidance inform the present document (the entire guidance is reproduced in Appendix 1):

- Personal data is information that relates to an identified or identifiable individual.
- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive, and you may only process them in more limited circumstances.
- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual, meaning clearly about a specific individual.

Applying this guidance to the APDS specifications, privacy relates to those attributes that may be used either separately or collectively to identify an individual. However, it may also include attributes that relate to a vehicle that can then be associated with an individual.

4. Definitions

The definitions of privacy, and the data that is relevant, vary widely depending on the source. For the purposes of this document, we have used the following definitions:

Data Privacy - the right of a person to expect that personal information about them is not retained, shared or communicated to others. Definitions of data privacy vary but usually include the right of an individual to set limits and conditions on the uses and disclosures that may be made of such information without their authorisation.

Data Protection - a set of strategies and processes that can be used to secure the privacy, availability, and integrity of personal data. Data Protection may be seen as an organisation's implementation of Data Privacy.

[1] For precise EU definitions see Article. 4(1) GDPR as well as Art. 9 and 10 GDPR which define sensitive types of personal data that need a higher level of protection.

Identifier, Descriptor, Attribute – terms that all describe a single item of information or data. These terms are used interchangeably in the source material used for this document. For example, the APDS specifications use the term 'Attribute', whereas the UK Information Commissioner's Office uses the term 'Identifier'. The term 'Attribute' is used as the default in this document except where the source material is quoted directly.

5. Legitimate use and consent

This document focuses on the nature and sharing of personal data and not on the ways in which an organisation can establish a valid legal ground for the use of personal information. However, establishing that ground is a key aspect of data the data protection rules. In Europe, GDPR allows an entity to use personal data on the basis of one or more reasons (see Grounds for Processing below). Article 6 of the GDPR provides an exhaustive list of the possible legal grounds for the lawful processing of personal data. Only one of these involves gaining the specific consent of the data subject[2]. In the United States the Driver's Privacy Protection Act defines a similar set of exemptions to the need for specific consent but the scope of the personal data is restricted to driver details originally obtained from a Department of Motor Vehicles source. An entity intending to collect and store personal data must ensure that it establishes a lawful ground to do this.

In a scenario where personal data is being shared however, the receiving party is relying on the sending party to have ensured that they have the right to collect, store and share the data. Any receiving party in this situation would be well advised to ensure that the data was obtained, stored and shared lawfully (especially, but not only, across border). Furthermore, the receiving party has to rely on its own lawful ground for the processing of the data it has received from the initial party.

6. Special categories of data

Under GDPR, some types of personal data are considered to need more protection because they are sensitive and may reveal more intimate details about a person[3]. This special category data, if misused, could create significant risks to the individual's fundamental rights and freedoms. Data that falls into the special category may relate to a person:

- health status,
- lifestyle,
- racial or ethnic origin
- political opinions
- religious and philosophical beliefs.

It also includes biometric and genetic data.

Whilst it may seem that data related to parking is unlikely to fall into one of the special categories, some data used to establish eligibility (e.g. membership of an organisation, entitlement to disabled parking) may be considered to do so. This includes the ability to infer details about someone so, for example it would be possible to infer that a person has a specific health condition if they hold a permit issued to oncology or dialysis patients. In the EU, it is necessary to rely on one of the

[2] It is important to note that pursuant to Article 7(3) GDPR a data subject has the right to withdraw his or her consent at any time. Consequently, the data controller must stop processing the personal data of the data subject concerned, unless the controller has another legal ground for processing of the subject's personal data.
[3] The categories of these data are defined in Article 9 and 10 GDPR. Lifestyle is not part of them unless it reveals a special category of data such as sex life or sexual orientation.

exceptions listed exhaustively in Article 9(2) GDPR in order to lift the general prohibition to process special categories of personal data.

7. Identifying an individual

Direct identification

There are 2 categories of data attributes that, either individually or collectively, may result in data falling within the data privacy scope. These are attributes that:

- Identify an individual (e.g. name, address, etc)
- Identify a specific vehicle (e.g. license plate used as a credential)

In most countries where GDPR applies, the license plate itself is considered personal data regardless of the fact that the vehicle may have been parked, or is being driven, by someone other than the owner.

Indirect identification

When direct information is combined with data relating to the location of a vehicle at a specific time, it is possible to infer more information about the individual. For example, a vehicle parked overnight in a hotel car park implies that the owner is staying at the hotel.

It is therefore important to also consider data that could be used, alongside other data, to indirectly identify an individual or vehicle. Some indirectly identifiable data characteristics may themselves fall under the 'special categories' of data.

An example would be where a trade union member who parks in a multi-story car park for work purposes benefits from a special rate, negotiated by the union for its members. As a result of this, the combination of vehicle owner and the use of the special rate could be used to identify that the individual using that vehicle is a union member.

A similar scenario could also be used to identify the religious beliefs of an individual who has a permit relating to a place of worship (e.g. a church, mosque etc.) if a local authority or religious group negotiate free or reduced rate parking for their congregation at times of worship. However, gathering license plate data regularly in a nearby public car park during worship times may also create data that could be used in the same way.

Another example of directly or indirectly identifiable information is the use of hanging tags to display a vehicle or person's credential. This is commonplace in certain parts of the world, North America for example, and may contain both directly and indirectly identifying information about the vehicle or its owner.

For car parks that allow visitors to reserve parking, the date, entry time, length of session, exit time and location of their vehicle may also be considered as sensitive information. This kind of data would allow someone who has access to it could be used to track someone's movements and predict the future movements of a vehicle or individual. Location data are particularly revealing of the life habits of an individual. The journeys carried out are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited[4].

[4] EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, see paragraph 63.

Indirectly identifying information could also include a vehicle parking in a bay reserved for employees or, in a hospital car park, spaces reserved for patients with a certain medical condition.

Personal information is not just for users of the car park. By way of example, the number used to identify parking enforcement officers is also a piece of indirectly identifiable information and in some jurisdictions, the advice is that parking enforcement companies should not include the issuing officer's ID number on a fine or citation.

Details of personal data specific to the APDS specifications is discussed below.

8. Key Concepts

The concepts used in the discussion of data privacy will vary between different jurisdictions and languages. Additional work will be required to 'map' terms across these boundaries.

Below is an initial list of the more common terms:

- **Data Subject** - An identified or identifiable natural person whose personal data are being processed.
- **Personal Data** - Any information relating to an identified or identifiable data subject
- **Data Controller** - An entity which determines the purposes and means of the processing of personal data
- **Data Processor** - An entity which processes personal data on behalf of a Data Controller
- **Data Processing** - Any operation or set of operations which is performed on personal data e.g. storage, structuring, use, disclosure etc.
- **Data Protection Agreement Or Data Privacy Agreement (DPA)** - An agreement between two data controllers or a data controller and a data processor to govern the processing of personal data (in the EU, in accordance with Article 28(3) GDPR).

9. APDS-Specific Data

The data that may be communicated using the APDS specifications includes a combination of personal data and non-personal data. The list below shows *at this time* which data may fall within the scope of personal data:

Domain	***Package***	***Class***	***Example attribute***	***When associated with***
Observation	Observation	image	image	
PkCommon	Contacts	ContactDetails	personFirstName, personName	
Quote	Quote	QuoteSessionExtensionRequest	suppliedCredential	
Rates	Eligibility		membershipName, Description	rightHolder,userQualification
Right	Right	AssignedRight	endValidUsagePeriod	
Right	Right	CustomerCredential	type, additionalInformation	
Right	Right	VehicleCredential		
Right	Right	Credential	type, additionalInformation	
Right	Right	OtherCredential	additionalInformation	
Right	Right	PlannedUse	estimatedStart, estimatedEnd	
Session	Session	Session	actualStart, actualEnd	
Observation	Observation		image, observedLocationTextual, startTime, endTime, observer	

Observation	Observation	Location	observedLocationTextual	
		ObservationElement	startTime, endTime, observedCredentialId,observer	

10. Rights and Responsibilities

Data subjects (e.g. drivers) may have rights under data privacy legislation, depending on jurisdiction. Data subjects who are in the EU, or who are outside the EU but whose data are processed by an organisation established in the EU, have the following rights under the GDPR:

- to be informed (Articles 13-14 GDPR)
- to access their data (Article 15 GDPR)
- to have their data rectified (Article 16 GDPR)
- to have their data erased (the so-called 'right to be forgotten') (Article 17 GDPR)
- to restrict the data processing (Article 18 GDPR)
- to data portability (Article 20)
- to object to the processing of their data (Article 21 GDPR)
- to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her (Article 22 GDPR).

It is to be noted that these rights are not absolute and subject to certain conditions and restrictions.

Similarly, data controllers have a number of obligations stemming from the GDPR. These include, among others, ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes, not more;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary;
- processed in a manner that ensures appropriate security.

Some jurisdictions have legislation relating to the transfer of personal data across international boundaries. The GDPR provides for several tools for transfers of personal data from the EU/EEA to non-EU/EEA countries. These tools include, among others, standard contractual clauses and adequacy decisions[5].

These rights and responsibilities flow from legislation in respective jurisdictions. Approaches to the standardisation of these concepts in the context of the APDS specifications is discussed in Section 14 below.

11. Lawful Grounds for Processing

For the processing of personal data to be lawful under the GDPR, it is mandatory for the controller to rely on one of the six possible grounds for processing which are exhaustively listed in Article 6(1) GDPR as follows:

- consent for specific purpose
- contractual obligation
- legal obligation of the data controller

[5] for more information, see: International dimension of data protection (europa.eu)

- protection of vital interest of the data subject or another natural person
- exercise of official authority or task in the public interest
- legitimate interest of the controller or a third party.

The determination of the lawful ground is crucial because the data subjects can exercise different rights depending on the lawful ground for the processing of their data.

One or more of these may apply for the commercial and operational situations covered by the APDS specifications.

However, it is necessary for one or both of the following to apply depending on the ground being relied upon:

1. The data subject has been informed.
2. The data subject has provided consent if consent is the lawful ground for the processing of the personal data pursuant to Article 6(1)(a) GDPR.

Consent

As stated above, consent is one of the 6 possible legal grounds for processing personal data. The consequence of using the consent is that the data subject can withdraw it at any time[6]. However, it is not necessary for the data subject to provide consent if the controller has another legal ground for the processing of personal data. In the parking context, it seems that 'contract', 'legal obligation' or 'legitimate interest' may be appropriate legal grounds.

12. Data Retention

As a general principle, personal data must not be kept for longer than it is needed for its original purpose. It is necessary to think about – and be able to justify – how long personal data is kept.

Article 5 (1)(e) of the GDPR states that personal data must be stored "*for no longer than is necessary for the purposes for which the personal data are processed.*". This is the *principle of storage limitation,* which means that personal data should only be kept long enough for it to be processed for its stated purpose. This period will vary depending on the reason you collect a particular type of log data. In order to comply with this principle, personal data should be deleted after it's been used to fulfil its stated purpose.

13. Use Cases

Some Use Cases will be provided in an Appendix to illustrate practical examples of the application of GDPR to parking.

14. Data Protection Agreements (DPAs)

It is customary for organisations to create bespoke data protection agreements (DPAs) between themselves and their suppliers.

[6] For more explanations on the requirements for obtaining and demonstrating valid consent under the GDPR, please consult the guidelines on consent of the European Data Protection Board (EDPB): edpb_guidelines_202005_consent_en.pdf (europa.eu)

In practice, an organisation may act as a Data Controller in one commercial relationship but may act as a Data Processor in another or may even act as both. Any APDS-related data protection agreements will need to recognise this.

There is an opportunity to create DPA templates to cover common data privacy relationships. Different legislation and practices in different jurisdictions may make it necessary to adopt a suite of template DPAs with the same core principles but differing in the necessary detail.

The European Commission has published standard contractual clauses that can be used by controllers for their data protection agreements with processors. See: Standard contractual clauses for controllers and processors in the EU/EEA (europa.eu)

Appendix 1: Identifying whether data is personal

How to identify whether data is personal can be found at https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

Appendix 2: Further sources of information

European Union Guidance

The following documents have been recommended as sources of information on data protection within the EU:

- EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)
- EDPB Guidelines 05/2020 on consent under Regulation 2016/679
- EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

© APDS 2025