Veri-park Data Protection

Data Protection Documentation 1.0

Data Protection Documentation - Veri-park
Issue March 2018

APT Controls Ltd

Maxted Corner
Maxted Road
Hemel Hempstead
HP2 7RA

Tel: +44 (0) 20 8421 2411
Fax: +44 (0) 20 8421 3951

Copyrights

Trademarks

Note

The information contained in this documentation has been put together with the greatest of care. Although this documentation is updated regularly, APT Controls Ltd. cannot guarantee the absolute correctness and completeness of the information contained herein.

Contents

1. About this documentation

This documentation explains important settings and technical solutions of Veri-park system. This documentation covers only selected procedures and does not claim to be complete. The procedures described in this manual do not cover troubleshooting. In case of problems, please send an accurate issue description to the Veri-park Support Team.

Symbols

Important text passages and notes are marked by symbols and special typefaces throughout this Manual. The following symbols are used:

CAUTION

Warns against actions that might cause hardware and/or software damage.

INFORMATION

This document contains important information about the proper handling of the device and its software.

EXAMPLE

Describes practical applications to illustrate features, functions, etc.

Warranty and liability

Except for all stipulated warranty and liability regulations, all warranty and liability claims shall be excluded, in particular if the harm or damage should be attributed to one or more of these instances:

- Misapplication (i.e., non-intended use) of the software
- Inappropriate installation
- Irregular or insufficient updating / upgrading
- Use of material not approved by APT Controls Ltd
- Failure to apply error correction measures recommended by APT Controls Ltd
- Insufficient training of operating personnel
- Minor errors that do not impair or limit the essential functions of the software
- Faults that do not fall within the liability of APT Controls Ltd
- Non-required changes made to the software by the principal or third parties without the written approval from APT Controls Ltd

- Failure to pay the full amount of the agreed-upon fee
- Damage caused by the actions of third parties, atmospheric discharges, unstable networks, chemical influences or Acts of God.

NOTE ON DATA PRIVACY

The operator is solely responsible for ensuring compliance with applicable legal requirements. As the operator, please ensure conformity with applicable (data protection) laws and legal requirements when configuring Veri-park system.

If in doubt, seek the assistance of your legal counsel and obtain the required authorisations from your customers where necessary.

CAUTION

This document refers to Central (VPC) and Local (VPL) components of Veri-park system developed and launched after the 25th of May 2018. APT Controls Ltd does not give any guarantee for Veri-park system components developed and launched before the 25th of May 2018 concerning the General Data Protection Regulation.

2. Introduction and definitions

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The GDPR replaces the data protection directive (officially Directive 95/46/EC) of 1995. It does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

DATA SUBJECT

A natural person whose data are being used, e.g. car owner, driver.

PERSONAL DATA

Personal data is every information which is bound to a natural person or can be used to identify a natural person. This includes name, address, phone number and this kind of information. Also data that can be used for identifying a natural person with a certain effort is considered as personal. This includes license plates (VRM).

DATA CONTROLLER

An organisation that collects personal data from EU residents, e.g. parking operator.

DATA PROCESSOR

An organisation that processes personal data on behalf of data controller e.g. cloud service providers, e.g. APT Controls Ltd. as a hosting partner.

The regulation applies if the data controller or processor or the data subject is based in the EU. Furthermore the regulation also applies to organisations based outside the European Union if they collect or process personal data of individuals located inside the EU.

The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonisation of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover.

What is new?

Significant sanctions and penalties of up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller.

Companies have to set up and maintain a list of processing activities and are ultimately responsible for compliance with the GDPR. The data protection authority has the right to audit companies at any time in order to verify their compliance.

Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request.

In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures which meet the principles of data protection by design and data protection by default. Privacy by design and by default require that data protection measures are designed into the development of business processes for products and services.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default and that technical and procedural measures should be taken care by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the GDPR regulation. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

The European Union Agency for Network and Information Security elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. An outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

Lawful basis for processing

Personal data can only be processed if there is at least one lawful basis to do so. The lawful bases for processing data are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- processing is necessary for compliance with a legal obligation to which the controller is subject,
- processing is necessary in order to protect the vital interests of the data subject or of another natural person,

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3. Rights of the affected person

A person affected by such a situation, that means a person whose data is being stored in a system, has certain rights, which can be forced onto the data controller.

Right of access (INFORMATION)

The right of access gives citizens the right to get access to their personal data and information about how this personal data is processed. A data controller has to provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore the data controller has to inform the data subject on details about the processing such as:

- what kind of data is stored,
- what actual data is stored,
- with whom the data is shared,
- how long the data is stored.

Right to rectification (CORRECTION)

The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure (DELETION)

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute “right to be forgotten”. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed,
- when the individual withdraws consent,
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing,
- the personal data was unlawfully processed (ie otherwise in breach of the GDPR),
- the personal data has to be erased in order to comply with a legal obligation,
- the personal data is processed in relation to the offer of information society services to a child.

EXAMPLE

A person cannot request the personal data to be deleted from a contract parking subscription for as long as the person is still using that contract, as the data is required to provide the underlying service.

Right to data portability (MIGRATION)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

COPY OF PERSONAL DATA

Data controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. Implementation in Veri-park system

APT Controls Ltd provides the means that the parking operator can adhere to the General Data Protection Regulation (GDPR). This applies to Veri-park system.

RECOMMENDATION

APT Controls Ltd highly recommends that every parking operator determines the exact procedure for his system with the help of an expert.

VERI-PARK SYSTEM TOPOLOGY

The Veri-park system topology contains two separate components which can store a personal data: Central (VPC) and Local (VPL). The data subject's rights are explained below from a perspective of these components.

Right of access (INFORMATION)

The data subject have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- what kind of data is stored,
- what actual data is stored,
- with whom the data is shared,
- how long the data is stored.

What kind of personal data is stored?

The following data objects (contain personal data) can be stored in Veri-park system:

- User Account (e-mail, forename, surname, address, phone number),
- Vehicle Record (number plate),
- Vehicles List (number plate),
- Sighting Image (number plate),
- Sighting Data (number plate),
- Parking Ticket (number plate),
- Payment History (number plate),
- Offence Record (number plate).

What actual personal data is stored?

NOTE

The request for information must be submitted within a month.

For information on actual personal data stored, the affected person has to contact the instance (e.g. parking operator) where personal data has been recorded first.

CONTRACT WITH PARKING OPERATOR

The affected person has a contract with a parking operator. For this contract, personal data has been stored.

CAUTION

An occasional parking entry is treated as a contract - the affected person should be informed about that fact via parking sign located near each parking entrance.

If the affected person wants to make use of the right for information, the affected person has to contact the parking operator with whom the affected person has a contract. The parking operator is obliged to provide the affected person with the requested information on personal data stored.

The parking operator prints the personal data stored in the Central Console of Veri-park system and hands the print-out over to the affected person.

- User Account details can be printed via the Print button available for user selected on “Users” page.
- Vehicle Record, Sighting Images, Sighting Data and Parking Ticket can be printed via Print button available for vehicle selected on “Search” page.
- Vehicles Lists on which a Vehicle Record exists can be printed via Print button on “Lists” page.
- Offence Record can be printed via Print button available for parking session selected on “Contraventions” page.
- Payment History can be printed via Print button available for payment record selected on “Reports/Payment Record” page.

FLEXI-PARK MEMBERS

The affected person is a Flexi-Park member.

WHAT’S FLEXI-PARK

Flexi-Park is the name of an automated pay-as-you-go service that parking operators can make available for their parkings through Veri-Park system.

If the affected person wants to make use of the right for information, the affected person has to login to Flexi-park website.

- User Account details are available on “Your personal details” page.
- Vehicle Records are available on “Manage vehicles” page.
- Parking Tickets are available on “Parking history” page.
- Payment History is available on “Payment history” page.
- Vehicles List, Sighting Image, Sighting Data and Offence Record are not available for Flexi-park members via the website. The affected person has to contact the Veri-park support team on e-mail: support@veripark.co.uk

With whom the personal data is shared?

The personal data is shared with parking operator and 3rd party companies which have permissions granted by parking operator.

RECOMMENDATION

APT Controls Ltd highly recommends that every parking operator sign a relevant contract with 3rd parties companies to whom is going to share personal data.

How long the data is stored?

Personal data is stored as long as an affected person has the contract with a parking operator. However, there are additional retention periods for number plates data stored in Veri-park system:

- Number plates data is stored locally on site server for 10 days,
- Number plates data is stored centrally on cloud servers for 100 days if there is no contraventions.
- In the case of contraventions, number plates are stored as long as required to finish contravention processing.

Right to rectification (CORRECTION)

The affected person can at any time request a correction of stored personal data, which has to be done accordingly. For the correction of actual personal data stored, the affected person has to contact the parking operator where the data was recorded.

The parking operator can correct personal data in the Central Console of Veri-park system:

- Vehicle List can be corrected on “Lists” page,
- Sightings Data can be corrected on “Search” page,
- Offence Record can be corrected on “Contraventions” page,

CAUTION

User Accounts, Vehicle Records, Sighting Images, Parking Tickets and Payment History can't be corrected by the parking operator

If the affected person is a Flexi-park member then some corrections can be made via Flexi-park website:

- User Account can be corrected on "Your personal details" page,
- Vehicle Record can be corrected on "Manage vehicles",

CAUTION

Vehicles Lists, Sighting Images, Sighting Data, Parking Tickets, Payment History and Offence Records can't be corrected by the affected person.

Right to erasure (DELETION)

The affected person can at any time request the deletion or removal of personal data where there is no compelling reason for its continued processing. This can only be done, if the requested deletion is not contradicting a purpose, e.g. the fulfilment of a contract the data is needed for.

There are two methods of executing the right to erasure:

- deletion of the dataset containing the personal data,
- anonymisation of the personal data on the dataset.

CAUTION

The only method of executing the right of erasure in Veri-park system is data anonymisation.

ANONYMISATION

"Anonymisation" of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

If the affected person wants to make use of the right for erasure, the affected person has to contact the parking operator with whom the affected person has a contract. The parking operator is obliged to delete personal data stored, if the affected person requests this.

The parking operator can anonymise user account and all related personal data via the Archive User button available for user selected on "Users" page.

If the affected person is a Flexi-park member then user account and all related personal data can be anonymised via Delete Account button available on “Your Personal Details” page of Flexi-park website.

Right to data portability (MIGRATION)

If the affected person wants to make use of the right for data migration - meaning that its data is exported to be used in another system - the affected person has to contact the parking operator, i.e. the instance where the personal data has been recorded first. The parking operator has to export the data for the affected person.

The parking operator can download user account and all related personal data via the Download Account Data button available for user selected on “Users” page.

If the affected person is a Flexi-park member then user account and all related personal data can be downloaded via Download Account Data button available on “Your Personal Details” page of Flexi-park website.