ANPR SOLUTIONS

GDPR Policy Notice

ANPR SOLUTIONS

Version 1.1
Thursday, July 12, 2018

CONFIDENTIAL DOCUMENT

ANPR SOLUTIONS

ANPR SOLUTIONS

TABLE OF CONTENTS

Introduction

The ANPRsolutions system

The ANPRsolutions system comprises of hardware, that is be deployed in the location where vehicles are being monitored, and the online software used for viewing, searching, automation, alerting and analysis.

This document provides a summary of our approach to data security and privacy in the context of the GDPR regulations.

Our privacy policy and our terms of use are available via our website.

Our software is marketed under the names:

ANPRsolutions
Private sector projects to monitor or control the movement of vehicles on private property. For example ANPR may be used for security, access control, car park management, safety and enforcement purposes.

SAFE-SPEED
Predominately aimed at the Parish councils to improve road safety in local communities by providing detailed traffic information on public roads.

SAFETYCAM
A speed monitoring application for closed road works to enforce contractor and employee safety on work sites.

Definitions

For simplicity, in this document, we will refer to the online software only as ANPRsolutions but the content of this document is relevant to all of the products above.

Number plates are also known as license plates or more technically as Vehicle Registration Marks (VRM) – we shall use VRM to refer to a number plate.

ANPR is short for Automatic Number Plate Recognition – the identification by software of a VRM in an image or series of images.

Data in ANPRsolutions

What data is held?

Event data

Generally we treat the recognition of a Vehicle Recognition Mark (VRM) as an event.

For each event we hold information derived from the live camera image usually by software residing on the local camera.

Event information always includes:

- The VRM
- The location (as pre-configured or via GPS)
- The time of the event

Event information may also include:

- The direction of travel
- The detected speed of vehicle as measured by radar
- A small thumbnail image of the vehicle
- An unaltered medium to high resolution image of the vehicle
- A medium to high resolution image of the vehicle with the plate highlighted

Derived data

Based on the event data, we optionally create and store additional data:

- Summary statistical data detailing traffic volumes and speeds broken down by hour and location.
- Occupancy data detailing how long vehicles spend on site or the average speed travelling between two points.
- Event outcomes such as authorized access, out of hours access, driving in the wrong in direction, exceeding speed limits and under or over staying time limits.

Configuration data

Some details are held about customers and their users with logins to the online software.. Customers can enter vehicle lists for access control or vehicle blacklisting.

Audit and logging data

User activity on the online software such as logins, searches and data exports, are logged to ensure that use of the system by authorised personnel can be reviewed.

How long is data held?

Data retention periods are configurable for different types of data. Required retention periods will vary by customer depending their answers to questions such as:

- How long do we retain single event data?
- How long do we store images?
- Do we store images for events not needed for the customer's stated purpose?
- At what resolution do we store images?
- How long do we retain derived data relating to occupancy?
- How long do we retain statistical information?

When our customers engage our services they specify how long they will need to keep data and why.

Examples:

- A valet car park may need to store images of the vehicles entering and exiting for 28 days as customers have 28 days to lodge a damage claim.
- A hospital car park may need to identify vehicles that are abusing their three-hour free parking restriction.
- Traffic statistics may need to be retained for two years to the monitor the increase in traffic caused by a new shopping centre.
- A recycling plant may need to keep details of truck visits for bulk billing.
- A parish council may need to keep a record of separate vehicle transits over several months to differentiate habitual speeders from non-habitual offenders.
- A factory may need to prove no unauthorized vehicles have been onsite this year.
- An airport may need to investigate any cargo vehicles visiting loading bays without first passing the control point.

Most sites need to retain up to a week's worth of data just to ensure the system has been working correctly.

Some customers may not need to retain high-resolution images of non-important events.

Customers wanting to keep event data for longer periods should have an explicit, specified and legitimate reason.

Some customers may be more interested in recent event data, so retaining full event data for long periods of time is unnecessary.

Customers may want to retain long-term statistic and analysis data as a business intelligence tool for on-going decision-making.

Do we hold personally identifiable data?

We do not consider a VRM alone to be personally identifiable data. The VRM identifies the number plate recognised on a particular vehicle. We do not ourselves have nor do we provide our customers any means to link a VRM to the registered owner or to the actual driver of the vehicle.

We also cannot verify that the VRM is on the vehicle it is registered to. Manual visual verification may be required on important event, such as speeding. This means that images relating to important events may need to be kept longer than images from non-important events.

If ANPRsolutions customers need to link a vehicle to an individual they would have to apply for personal data via the appropriate procedures as mandated by the vehicle registry authority.

We do not explicitly provide a function for any personal related information to be manually linked to an event and stored in our system.

How is data held?

All our data is securely held in online storage within the same legislative region as where the data was collected and where the customer resides.

Direct and programmatic access to data is restricted and controlled using industry standard security and encryption.

Access security credentials are limited to authorised personnel and are regularly changed.

Web access to the application is only available only over a SSL connection using authorised credentials with strong, enforced password policies. Customers are responsible for the maintenance of user access to their own data via our online software.

Recommended site installations use encrypted virtual private networks (VPNs) over public or private connections to transmit data between the site and the online software.

Our remote hardware is physically and virtually secured.

All third party software is regularly updated with any available relevant security patches.

Who is data shared with?

Our customers own and are responsible for their data.

Customers can choose to share their data with third parties either by automatically or manually sending the data on or by providing them access logins to our online software. For example car parks may need to share their data with a payment company to take parking payments or councils may share their data with the police to alert them to traffic incidents. Customers that do this should be aware of their obligations with regards to the privacy of individuals.

Customers can extract data in the form of PDF reports, spread-sheets or archives. Data extracted from the system ceases to be our responsibility and customers need to ensure that extracted data is reasonably protected.

We do not sell the customer's data to third parties.

Data subject's rights

Individuals may use theirs rights as possible data subjects to request access from our customers to data kept in the online software.

However, there is no means of linking an individual to a particular event. Such a request would require the individual to provide proof that they were actually driving, or a passenger of the vehicle involved in an event, and that they had permission of anyone else that may have been involved in the same event.

If the owner of a particular VRM could adequately prove that they are the registered vehicle owner and were also the driver of the vehicle for the period in question, then the customer may decide there are sufficient grounds to provide access to the relevant data. Our system provides the means for the customer to provide that data directly as they see fit.

For example, a vehicle owner may ask to see images or data relating to speeding offences captured by a council. The council may not automatically release the data, as that could affect the privacy of the actual driver or other passengers of the vehicle. The owner would need to provide evidence, or an affidavit, that they were the owner and the driver (or had the driver's permission).

The deletion or rectification of data would only be done by us on the direct request of the customer, the courts or any statutory authority with the legal rights to do so - normally following a request from a data subject who has previously proven their identity. It is not our responsibility to respond to such requests directly, but we would refer any direct requests back to the customer and ask that they respond in a timely manner.

Our customer's responsibilities

We provide our customers with an online service and hardware in relation to specific requirements.

Our customers have several responsibilities that they agree to when using our system:

- To completely, and accurately, keep us informed of the legitimate purpose(s) for the storage and usage of data collected on their behalf.
- To ensure that the data retention policies reflect the stated purpose(s).
- To ensure that potential data subjects are adequately informed that they are possibly subject to ANPR and video surveillance
- To provide potential data subjects a means to contact the customer for more information.
- To maintain their own data privacy and GDPR procedures for the use and handling of data and data access requests.
- To ensure online access is limited to current authorised users, that authorised users keep their security credentials secure and that the system is only used for legitimate purposes.
- To consider and respond to data requests according to any relevant legislative requirements in a timely fashion

The full terms of use that our customers agree to are available on request.

Our responsibilities

We are the caretakers of customer's data.

We have responsibilities to our customers and to any potential data subjects:

- To keep our privacy policies and terms of use up to date, accessible and simple.
- To keep data secure from all forms of unauthorised access.
- To keep data secure from accidental loss.
- To provide our customers with the tools to control and access their data.
- To provide our customers with data retention periods that can be customised on request.
- To provide our customers with the tools to respond to data access and rectification requests
- To action any data deletion requests submitted by the customer.
- To consider any relevant legislative requirements when providing software services to our customers.
- To maintain and regularly review internal procedures for the protection of data, the detection of any data theft or loss and the dissemination of information relating any data incidents.
- To register with any relevant data protection authorities.