Tástáil Ródacmhainneachta um Fheithiclí Tráchtála
Commercial Vehicle Roadworthiness Testing

Commercial Vehicle Mobile ANPR Policy

Road Safety Authority – May 2015

Mobile ANPR System Data Protection Policy

This document sets out the policy of the Road Safety Authority (the "**Authority**") regarding the use of a mobile automatic number plate recognition ("**Mobile ANPR**") system in connection with commercial vehicle roadworthiness ("**CVR**") and drivers' hours roadside inspections. It describes the steps to be taken to ensure that images and information processed by such a system are collected and used in a manner that complies with the Data Protection Acts 1988 and 2003 (the "**DPA**").

This policy applies to all employees, agents and contractors of the Authority ("**Authority Personnel**"). A failure by any Authority Personnel to comply with this policy may result in the relevant person being subject to disciplinary action, up to and including summary dismissal or termination of contract, as applicable.

Background

The Authority is a statutory body established under the Road Safety Authority Act 2006 with various statutory functions and powers connected with road safety. Under the Road Safety Authority (Commercial Vehicle Roadworthiness) Act 2012 and related Regulations, these include monitoring the compliance of commercial vehicles that are subject to the CVR regime ("**CVR Vehicles**") and the owners and operators of such vehicles with applicable statutory obligations in connection with vehicle roadworthiness, maintenance and repair by carrying out roadside inspections. Under the Road Safety Act 2006, the European Communities (Road Transport) (Working Conditions and Road Safety) Regulations 2008, as amended, and related Orders and Regulations, the Authority's statutory functions and powers also include the development, operation, oversight and delivery of targeted and random roadside testing in connection with, among other things, rules governing drivers' hours and tachograph, breaks and rest periods ("**Drivers' Hours Rules**"). In order for the Authority to be in a position to perform these functions in an effective and efficient manner, the Authority has decided to use a Mobile ANPR system at roadside inspection checkpoints to assist with identifying CVR Vehicles and, in particular, CVR Vehicles that are on any watch list maintained by the Authority in connection with its CVR, Drivers' Hours and digital tachograph activities (a "**Watch List**"). Please see the appendix to this policy for a technical description of the proposed Mobile ANPR system.

As a result of the operation of Mobile ANPR cameras at roadside inspection checkpoints, an image of the number plate of each vehicle that passes such a camera while it is operating will be taken. The number plate and related data, such as the time at which the image was taken, will then be transmitted via a secure transmission system to CoVIS (which is the main software solution used by the Authority in connection with its CVR activities). For the purpose of the DPA, the number plate data that is collected or otherwise processed by the Authority may constitute 'personal data', if an individual can be identified from that number plate in conjunction with other information that is in, or is likely to come into, the possession of the Authority (e.g. by linking it with other information held by the Authority relating to the relevant CVR Vehicle, such as the name of the registered owner of that CVR Vehicle). Although not all number plates that are collected by the Authority via Mobile ANPR cameras will constitute 'personal data', some will. The Authority is a 'data controller' of any personal data that is collected or processed via its Mobile ANPR system ("**Mobile ANPR Personal Data**"). The Authority requires Authority Personnel to take the steps described below to comply with the key principles under the DPA in respect of the processing of such personal data.

1. Obtain and process personal data fairly (section 2(1)(a) of the DPA)

For personal data to be obtained fairly, a data controller must ensure that, so far as is practicable, data subjects are provided with, or are otherwise aware of, certain information at the time at which their personal data is obtained. Since the use of Mobile ANPR cameras at roadside inspection checkpoints will involve the collection of personal data, appropriate signage must be displayed next to such cameras to make approaching drivers aware of their presence and operation.

For personal data to be processed fairly in this context, save where an exemption applies, the Authority must be in a position to rely on one of a range of 'legitimising conditions' that are set out in the DPA. One such legitimising condition is where the data subject has consented to the processing. The DPA also provides for alternative legitimising conditions. The Authority's general practice is to seek to ensure

that, in connection with the processing of Mobile ANPR Personal Data, it is in a position to rely on one of the following legitimising conditions:

- that the processing is necessary for the performance of a function conferred on the Authority by applicable legislation (pursuant to section 2A(1)(c)(ii) of the DPA); and/or

- that the processing is necessary for the purposes of the legitimate interests pursued by the Authority and is not unwarranted by reason of prejudice to the fundamental rights and freedoms or legitimate interests of data subjects (pursuant to section 2A(1)(d) of the DPA).

2. Obtain personal data only for one or more specified, explicit and lawful purposes (Section 2(1)(c)(i) of the DPA)

Mobile ANPR Personal Data is obtained for the purposes of the Authority performing its CVR, Drivers' Hours and other road transport law monitoring and enforcement functions, including the implementation of a risk rating system in respect of CVR Vehicles, and for purposes reasonably incidental thereto including, without limitation:

- identifying which of the vehicles that approach a roadside inspection checkpoint are CVR Vehicles;

- identifying which of the CVR Vehicles that approach a roadside inspection checkpoint are on a Watch List and assisting Authority personnel and Gardaí at the checkpoint in deciding which CVR Vehicles should be stopped and inspected and which should be allowed to pass through the checkpoint;

- monitoring the compliance of owners and operators of CVR Vehicles with applicable statutory obligations in connection with road transport and vehicle roadworthiness, maintenance and repair;

- monitoring compliance with Drivers' Hours Rules;

- investigating and, if necessary, taking appropriate enforcement actions in respect of CVR Vehicles whose condition or operation is not compliant with applicable statutory obligations in connection with road transport and vehicle roadworthiness, maintenance and repair;

- investigating and, if necessary, taking appropriate enforcement actions in respect of non-compliance with Drivers' Hours Rules; and

- recording and analysing general statistics regarding the performance by the Authority of its CVR, Drivers' Hours and other road transport law functions and general levels of compliance with CVR, Drivers' Hours and other road transport law obligations.

3. Use and disclose personal data only in ways compatible with the purposes for which it was collected (Section 2(1)(c)(ii) of the DPA)

Mobile ANPR Personal Data may be used by or on behalf of the Authority for the purposes set out in Section 2 above. For example, it may be used by Authority Personnel to implement and administer the risk rating system that applies to CVR Vehicles and/or to identify an instance of non-compliance of a CVR Vehicle with applicable CVR obligations. In addition, it may be disclosed to relevant third parties for such purposes. For example, Authority Personnel will disclose such data to Gardaí, including but not limited to Gardaí at roadside checkpoints, where this is required for the purpose of the prevention, detection or investigation of a criminal offence, improving the efficiency of roadside checks, increasing deterrence of non-compliance with road transport and safety law, increasing public confidence in road safety and reducing traffic accidents. Such data may also be disclosed to other public bodies, such as the National Roads

Authority, where necessary or relevant to the purposes set out in Section 2 above or as otherwise permitted or required by law.

Save as otherwise permitted by the DPA, Mobile ANPR Personal Data is not to be used or disclosed for any other purpose.

4. Keep personal data safe and secure (Section 2(1)(d) of the DPA)

The Authority takes appropriate operational and technical security measures against unauthorised access to, or alteration, disclosure or deletion of, Mobile ANPR Personal Data, including the following:

- Access Restricted on a 'Need to Know' Basis: Access to Mobile ANPR Personal Data is restricted to Authority Personnel who require access to it in order to perform the responsibilities assigned to them by the Authority, via appropriate password and identification authentication procedures.

- Storage: Mobile ANPR Personal Data is not permanently stored on Mobile ANPR cameras. The number plate of a passing vehicle that is captured by a Mobile ANPR camera and related data is transmitted in encrypted format to CoVIS and, to the extent that it is retained on CoVIS, it is hosted by a third party on the Authority's behalf on secure servers at a data centre which meets or exceeds TIA-942 Tier level 3 requirements.

- Unauthorised Disclosure: Mobile ANPR Personal Data may not be disclosed to any third party without the approval of RSA Data Protection Officer.

- Third Party Processing: To the extent that any third party processes Mobile ANPR Personal Data (or any other personal data) on behalf of the Authority, the Authority's practice is to ensure that there is a written agreement in place which includes, amongst other things, appropriate security obligations regarding such processing.

5. Keep it accurate, complete and up-to-date (Section 2(1)(b) of the DPA)

The Authority endeavours at all times to ensure that all personal data it holds is accurate, complete and up to date to the greatest extent practicable. In respect of Mobile ANPR Personal Data, appropriate security measures are taken to prevent any unauthorised alteration of it.

6. Ensure that personal data is adequate, relevant and not excessive (section 2(1)(c)(iii) of the DPA)

The Authority endeavours to ensure that any personal data obtained and processed in connection with roadside inspections is adequate, relevant and not excessive by, amongst other things:

- minimising the extent to which personal data that is not related to CVR, Drivers' Hours Rules and other road transport law monitoring and enforcement is collected or held by the Authority via its Mobile ANPR system to the greatest extent possible, including by promptly deleting number plates and related data that have been captured by Mobile ANPR cameras where they do not match any number plate on the master database of CVR Vehicles that is maintained by the Authority; and

- only collecting and using the minimum amount of personal data that is necessary for the performance of the Authority's CVR, Drivers' Hours Rules and other road transport law monitoring, investigation and enforcement functions.

7. Retain personal data for no longer than is necessary for the purpose(s) for which it was collected (Section 2(1)(c)(iv) of the DPA)

Number plates of passing vehicles that are captured by Mobile ANPR cameras at a roadside inspection checkpoint and related data are transmitted via a secure transmission system to CoVIS and automatically checked against the Authority's master database of CVR Vehicles. Any number plate that does not match a number plate on this database is promptly and irretrievably deleted. Only data relevant to numbers plates that are on the CVR Vehicle database are retained. The Authority does not retain data relevant to numbers plates of CVR Vehicles captured by Mobile ANPR cameras at roadside inspection checkpoints for longer than 3 years, save where they are required to be retained for a longer period for the purposes referred to in section 2 above (e.g. in connection with ongoing investigations or enforcement proceedings).

8. Give a copy of his/her personal data to an individual, on request (Section 4 of the DPA).

Under Section 4 of the DPA, subject to certain exceptions, an individual has a right of access to personal data relating to them which is held by a data controller. If an individual makes a request in accordance with Section 4 for access to Mobile ANPR Personal Data relating to him/her which is held by or on behalf of the Authority, the Authority will provide the individual with access to such data to the extent that it is required to do so under the DPA.

9. Address Personal Data Security Breaches

For the purpose of the Personal Data Security Breach Code of Practice that was published by the Data Protection Commissioner in 2010, the Authority maintains a log of all incidents which give rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data in respect of which the Authority is a data controller. Where necessary, the Authority will notify affected data subjects, appropriate enforcement authorities and/or the Data Protection Commissioner of such incidents.

It is essential that all incidents which give rise to a risk of unauthorised disclosure, loss, destruction or alteration of Mobile ANPR Personal Data are reported without delay to RSA Data Protection Officer. Such incidents may range from relatively minor incidents, which do not actually result in unauthorised disclosure, loss, destruction or alteration of personal data, to major security incidents, such as the loss or theft of devices or media which contain Mobile ANPR Personal Data.

Appendix – Mobile ANPR Specification

The Mobile ANPR camera will be setup within, or close to, the checkpoint controlled area. The set up location will be determined so as to enable sufficient time for the processing of messages and ANPR plate reads. The location and efficiencies of plate reads will be one of the operational parameters established via the working Mobile ANPR pilot.

The Mobile ANPR camera will send a plate read for each vehicle and this will be passed to a central processing CoVIS module. This module will determine if the passing vehicle is a CVR vehicle and also if that CVR vehicle is on a watch list. If it is then the system will send a notification to the officers at the checkpoint. Currently it is proposed to do this via the officers smartphone which will be associated with the checkpoint.

Following a receipt of this notification the officer will, and only where it is safe to do so, attempt to 'bring' the vehicle into the checkpoint so that an inspection can be carried out.