UNIVERSITY OF TARTU
SCHOOL OF LAW

Joonas Põder, Rando Mändar, Mehis Lõhmus

DATA PROTECTION LAWS AND PUBLIC USE OF COLLECTED TRAFFIC VIDEO DATA

Thesis

Supervisor
Magister Juris Karmen Turk

Tartu
2020
# TABLE OF CONTENTS

ABSTRACT ........................................................................................................................................ 3

1 THE CONTROLLERS AND/OR PROCESSORS OF DATA COLLECTED IN TRAFFIC ........................................................................................................ 4

1.1 Private data controllers .................................................................................................................. 4
1.2 Public data controllers ..................................................................................................................... 5

2 DATA COLLECTED BY SMARTPHONES, DASH CAMS AND ADAS .................. 6

2.1 Data collected by smartphones .................................................................................................... 6
2.1.1 Data collected by smartphone cameras .................................................................................. 7
2.1.2 Data collected by smartphone microphones ......................................................................... 8
2.1.3 Data collected by smartphone location detecting devices ...................................................... 9
2.2 Data collected by dash cams ......................................................................................................... 10
2.3 Data collected by ADAS ................................................................................................................. 11

3 LEGAL ANALYSIS OF TRAFFIC VIDEO DATA PROCESSING ...................... 12

3.1 Legal grounds for traffic video data processing .......................................................................... 12
3.1.1 Legitimate interest as a legal ground for data processing ....................................................... 14
3.2 Drivers as Controllers of the Dash Cam video data .................................................................. 17
3.3 Legal grounds for sharing the recordings ..................................................................................... 17
3.4 Processing special category data .................................................................................................. 20

4 SOLUTIONS ON HOW TO COLLECT TRAFFIC VIDEO DATA IN COMPLIANCE WITH GDPR .................................................................................. 22

CONCLUSION ................................................................................................................................. 24

REFERENCE LIST .......................................................................................................................... 26
ABSTRACT

When determining the legal context of data processing, the nature of said data processing should first be identified - different data controllers have different interests in the processing of data. The nature of these interests could influence the legality of data processing. These uses for the relevant data and their legal significance shall be explored further in section 1 of this paper.

In order to analyze the effects and legal backdrop of using data gathered and provided to processors by individual drivers using their mobile phones, dashcams or ADAS, the kinds of data that they collect must be identified and classified according to their legal significance - does collecting certain kinds of data even have potential legal consequences? Thus, this paper, in section 2, sets out to map out the categories of data collected.

Finally, in section 3, this paper sets out to combine the purposes behind the data collection, either in public or private interests, with the category of data they are interested in processing and assessing whether such data processing would be legal under the existing European Union and Estonian legal framework. Should it be found that the grounds for processing data either for the aforementioned public or private purposes are lacking, potential solutions for overcoming the shortcomings shall be proposed.

All relevant analysis will be conducted through the lens of the General Data Protection Regulation, the ePrivacy Directive and relevant Estonian regulations.
THE CONTROLLERS AND/OR PROCESSORS OF DATA COLLECTED IN TRAFFIC

Very bluntly put, parties interested in collecting data on massive scales, including traffic data, fall into one of the two following categories:

1) Public actors interested in fulfilling the functions given to them by the state legislator;
2) Private actors interested in fulfilling the functions given to them by private persons.

For the sake of simplicity non-governmental organizations shall be excluded from this list, as there may be overlap between their goals and the goals of public institutions. The instructions provided for this paper did not reference any such organizations specifically.

1.1 Private data controllers

Non-NGO private actors, in processing data potentially gathered from dashcams, drivers’ smartphones or ADAS systems, may be presumed to be acting with the purpose of maximizing income from the services they offer or to lowering costs related to offering said services. Insurance providers, for example, would most likely be interested in using potentially accessible data to conduct general risk assessment analysis or to attempt to refuse insurance claims in individual cases.\(^1\) Private actors could attempt to gather the data from drivers either via their consent or by contractual means, \textit{i.e.} obliging their customers to provide them with data as a part of a service agreement between the parties. This would make the private actors the controllers of the data within the meaning of GDPR art 4 subsection 7 and the persons providing them said data both the processors of the data in the sense of GDPR art 4 subsection 8, since they gather and forward data about other data subjects to the relevant private actors, and data subjects in the sense of GDPR art 4 subsection 1, as any recordings would also provide data regarding the person providing it, \textit{e.g.} their location and identity etc. Any further legal analysis must, therefore, take into account the legal consequences of using motorists as a source of data.

1.2 Public data controllers

Public institutions, such as the police, would either be interested in processing traffic data to redesign roads, advise lawmakers in drafting regulation or perhaps to have the legislator institute a punitive and/or preemptive traffic control system, such as the UK penalty point system,\(^2\) and to use the data collected in traffic in its implementation. The above uses of collected traffic data would serve both the goals of increasing general logistical efficiency and public safety. An increase in road safety may result in the loss of fewer lives in traffic accidents and as such may be considered the most significant and convincing argument for the processing of data gathered on the roads. Of course, the quantitative effect of such data processing on road safety is relevant in assessing its proportionality - if the positive effect the data processing would be marginal, then relying on proportionality as part of its legal basis would likely not work out in favor of the data controller. However, any such assessment would fall outside the scope of this paper, and in order to give academic purpose to this paper, it shall be assumed that any such improvements to road safety have been assessed to result in significantly less accidents and more lives saved.

As with private data controllers, so with public data controllers it must be taken into account that the persons collecting the data, everyday motorists, will become data processors on their behalf. The legal implications of this must be taken into account in conducting further analysis.

2 DATA COLLECTED BY SMARTPHONES, DASH CAMS AND ADAS

In order for data collected to have a legal significance, it must contain personal data in the sense of GDPR art 4 subsection 1, meaning any information relating to an identified or identifiable person. When it comes to video footage and other recordings made in traffic, several kinds of data may be encountered within it, including personal data and possibly even special category personal data.

For the purposes of this paper, the different sensory equipment attached to devices used by individuals to monitor the roads and their functionality shall be briefly explained, and the different kinds of data they may be able to provide a data controller shall be categorized as either non-personal data, personal data, or special category data in the sense of art 9 of the GDPR.

2.1 Data collected by smartphones

Smartphones on the whole are likely the most versatile of the three devices, as they are designed to contain a wide array of sensors. They may contain accelerometers, gyroscopes, magnetometers, GPS, proximity sensors, ambient light sensors, microphones, touchscreen sensors, fingerprint sensors, pedometers, barcode or QR code sensors, barometers, heart rate sensors, thermometers, air humidity sensors or even Geiger counters in the case of a model of smartphones released in Japan. All of these combined can give very detailed information about the person using them and their whereabouts, even if certain functionalities are switched off. For example, gathering data from a smartphone’s accelerometer, barometer and magnetometer and comparing it to weather data and geological survey maps, can be used to pinpoint the location of the user of a smartphone without the use of GPS systems.

At this point, assumptions must be made regarding how a smartphone would be used in monitoring traffic. A good way to discern what functions may be deemed necessary to be used in traffic in lieu of dash cams, would be to compare them to dash cams. However, even dash cams have variability, so any such comparison would not sufficiently discern useful and non-useful functions. Even so,

---

many functionalities of smartphones that might prove useful in traffic recordings may have been excluded from dash cams for mitigating production costs. All potentially useful functionalities of smartphones should be addressed in discerning the kinds of data they collect and forward to data controllers, however, doing so in this paper would be overambitious. For this paper, data from smartphone cameras, microphones, locating devices shall be addressed.

### 2.1.1 Data collected by smartphone cameras

It is clear that the most useful data to gather is likely visual - vehicles, their potentially dangerous maneuvers and their registration numbers would most likely be identified by visual means, hence, any smartphone used by drivers to gather data must have its camera turned on.

Video footage captures a multitude of different data in public, including, most importantly, people and vehicles. According to GDPR art 4 subsection 1, personal data is any information relating to an identified or identifiable natural person, meaning that if data can lead to the identification of a natural person, it is personal data. This, inter alia, includes the faces of pedestrians, people in vehicles and vehicle registration numbers, which could be captured.

It could be argued that capturing video footage could result in processing special categories of personal data, should any of the data listed in art 9 subsection 1 of the GDPR be recorded. According to recital 51 of the GDPR: “The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.”

The regulation is unclear on what exactly constitutes a specific technical means and whether high-resolution smartphone cameras, potentially ubiquitous in the near future, may be considered such specific technical means. It is likely, that high-resolution smartphone cameras are to be considered such specific technical means if they can be used to uniquely identify or authenticate a natural
person - which they already are capable of doing via iris scanning and facial recognition. Iris scanning and facial recognition are only two of many methods of visual identification, which may in the future become widely used; these include identification by the shape of a person’s ear, retina recognition, fingerprint recognition (e.g. if left on windshield) and finger and hand geometry recognition.

Although within the contemporary legal context, there is no use in defying recital 51 of the GDPR and considering photographs to carry special category data, it is likely that this stance will change or be updated in its interpretation, as hardware capable of capturing high-resolution footage and software capable of identifying persons from afar becomes more widespread. Staying firm to the position that photographs may not be considered to contain biometric data does not serve the explicit purpose of considering biometric data special category data as laid out in art 9 subsection 1 of the GDPR, because it is clear that biometric data can be extracted from mere photographs. Visual data concerning natural persons can be considered as both personal data and special category data in the sense of art 9 subsection 1 of the GDPR.

2.1.2 Data collected by smartphone microphones

Auditory data can be useful in potential traffic disputes - data gathered with microphones can give insight into the technical condition of the vehicle it is situated in (for example, a broken tire may not be visible from inside the vehicle, but will likely be heard), the condition of the driver, for example if the driver is speaking on the phone or slurring their speech, indicating intoxication) or traffic events out of the field of vision of the camera, such as impacts under the vehicle.

The same problem that arose with visual footage, arises with voice recordings - they may contain biometric data in the sense of art 9 subsection 1 of the GDPR. Similarly to eyes or ears, a person’s

---

voice can be used to identify them,\textsuperscript{9} meaning that, strictly speaking, a voice recording of a person can be considered biometric data. Voice recordings have been considered by EU member state authorities to be biometric data.\textsuperscript{10}

Any overhead conversations may also contain other special category data, including, for example, data concerning the data subjects’ political beliefs or sexual behavior. A likely counterclaim is that any microphone will only record only the interior of the vehicle, but this point is moot, as a driver that would potentially give explicit permission to process their special category data as per GDPR art 9 subsection 2 point 1, may also have passengers who have not done so in their vehicle.

Unlike with visual data, no part of the GDPR excludes or attempts to exclude the classification of audio recordings under special category data. As such any controller working with audio data collected from vehicles must take into account that they are bound to contain special category data in the meaning of art 9 subsection 1 of the GDPR.

\subsection*{2.1.3 Data collected by smartphone location detecting devices}

Movement and location of a smartphone user can be tracked using several methods - by GPS and WiFi,\textsuperscript{11} accelerometers\textsuperscript{12} or by different combinations of data.\textsuperscript{13} For the purposes of this paper, all of the aforementioned methods and corresponding data shall be concentrated to signify location data as such.

Location data is likely to be gathered by drivers using smartphones for monitoring traffic, as it can help avoid any confusion as to the location of a potential accident, vehicle speed and movement

\begin{thebibliography}{9}
\end{thebibliography}
direction. All of this data is vital in assessing the driver’s conduct in traffic and makes any potential disputes easier to solve.

Unlike video footage and audio recordings, deriving special category data in the meaning of art 9 subsection 1 of the GDPR from location data is difficult, but not strictly impossible. Should a data subject, for example, make regular visits to specific health clinics, it could be concluded that they may have a certain type of medical condition. Any data that would allow a data controller to, with sufficient certainty, gain insight into a data subject’s special category data without extensive efforts, could be considered special category data. The GDPR does not provide for a provision explicitly supporting a contrary interpretation, unlike in the case of photographs. However, since location data alone leaves much room for speculation and requires additional data to cross-reference in order to draw sufficiently certain conclusions, for the purposes of this paper, it shall be considered mere personal data.

2.2 Data collected by dash cams

Although more specific in their function, dash cams still vary in their features. They may be external or internal to the vehicle. Their field of vision may be restricted to the outside, but they may also have a 360 degree scope of the inside of the vehicle. Generally, they work by capturing footage, saving it on a data container, and, when the data container becomes full, overwriting older data. Usually, they have at least microphones, cameras and GPS systems for data recording purposes. Some also have Wi-Fi, Bluetooth or 4G capabilities for the purpose of gathering data.

Similarly to smartphones, the data collected by dash cams mostly originates from camera footage, microphone recordings and devices that could be used to locate the user. Hence, the same kind of data is gathered via dash cams, as is gathered using smartphones - visual data, that currently is not considered to be special category data, auditory data, that is likely to contain special category data, and location data, that more likely does not contain special category data.
2.3 Data collected by ADAS

ADAS or advanced driver-assistance systems are systems in vehicles that help the vehicle driver while driving or parking. They are combinations of different devices that either have an output, e.g. notify the driver of an event, or collect and process data to provide the aforementioned output. These systems rely on different data inputs, like video, LiDAR, radar and Wi-Fi or other methods to interact with other vehicles in their proximity. Breathalyzer sensors to prevent drunk driving and infrared lights to prevent accidents from drowsiness have also been proposed.\(^{14}\) Even the seatbelt sensor is part of ADAS systems.

As with both smartphones and dash cams, there is variety between ADAS devices and no fixed standard exists. While devices like LiDAR and radar have different technical capabilities to sensors widely used in dash cams and smartphones, ADAS systems do not gather personal data significantly different from those gathered by smartphones or dash cams. The types of data gathered can largely still be categorized as visual, auditory and location data, and as such the types of data include both special category data and mere personal data.

3 LEGAL ANALYSIS OF TRAFFIC VIDEO DATA PROCESSING

Traffic video recording devices are subject to General Data Protection Regulation in certain circumstances which gives the need to analyze the public use of collected traffic video data as most of the traffic video data is captured by dash cams, smartphones and ADAS systems.\(^{15}\)

Recordings usually contain images of identifiable individuals, their cars, license plate numbers and their voices as well and they are all “personal data” in the means of General Data Protection Regulation.

Not all the dash cams used are subject to General Data Protection Regulation. If the footage is kept for themselves and not published, then the household exemption applies and there is no need for compliance with the General Data Protection Regulation.\(^{16}\) If the footage is used for other purposes, then the use has to be compliant with General Data Protection Regulation. This is usually assessed on a case by case basis.

3.1 Legal grounds for traffic video data processing

Personally Identifiable Information (PII) (e.g. age, race, social security number, address, etc.) plays a vital role in providing user-centric services. Many IT companies collect, store and process PII of their customers by means of various mobile applications.\(^{17}\)

A tech-security company Gemalto's Breach Level Index (BLI) 2017 revealed that an avg. 10.4 million PII evidence are exposed each day where 74% were identity theft. To deal with such problems, many countries and organizations initiated to reduce personal data breaching. For instance, European General Data Protection Regulation (EU-GDPR), Australia's Privacy Amendment, Personal Information Protection and Electronic Documents Act by Canada,


\(^{16}\) P. Aurelija, 2019.

ISO27001 by International Organization for Standardization have been proposed to control personal data collection process.¹⁸

There is a saying in Lithuania that instead of hearing a hundred times it is better to see once. Visual means convey the most information and that is why filming devices are the best tools to collect accurate data. Along with the development of image capturing devices and other technologies, concerns about data subjects’ privacy grows. The fact that the EU found the enactment of the GDPR to be necessary indicates that people’s private information had been in danger. The same applies to filming traffic video data with dash cams, smartphones or ADAS systems.¹⁹

Under EU law, consent as a basis for lawful data processing is firmly established in Article 6 of the GDPR and is also explicitly referred to in Article 8 of the Charter.²⁰ A large part of the GDPR regulates data processing, which is based on the data subject's consent. But in case of dash-cams, smartphones which are used as dash-cams and ADAS, it is not practically possible to ask consent from all the people whose data is being processed by the aforementioned devices. Usually the data subjects will never know that their face or car registration plate or activities were filmed by a bypassing cars’ dashcams. Therefore, legal grounds for data processing other than consent must be analyzed.

Said lawful grounds for processing according to the GDPR art 6 are:

1) Necessity for the performance of a contract art 6 (1) (b)
2) Legal duties of the controller art 6 (1) (c)
3) Vital interests of the data subject or those of another natural person art 6 (1) (d)
4) Public interest and exercise of official authority art 6 (1) (e)
5) Legitimate interests pursued by the controller or by a third-party art 6 (1) (f)

When a dashcam device is used by a person, the legal basis for the use and storage of the video data are quite narrow. Necessity for the performance of a contract, which also covers pre-

¹⁸ H. Onik. Ibid, pg 71.
contractual relationships\textsuperscript{21} cannot be practically used as a legal ground for dashcam video processing since there is no contract between the data processor and the person who is being filmed (data subjects). Using a dashcam while driving is not a legal obligation. It is everyone’s free choice whether they want to use the device or not and therefore collecting video data cannot be considered as a legal obligation according to GDPR art 6 (1) (c). Whether dashcam videos can be processed based on the vital interests of the data subject or those of another natural person is questionable. This legitimate ground may only be invoked for processing personal data based on the vital interests of another natural person, if such processing “cannot be manifestly based on another legal basis”.\textsuperscript{22} Public interest and the exercise of official authority as a legal basis for dashcam video processing can only be used by state officials or people who exercise public authority. Private individuals who do not exercise official authority cannot rely on this exception. The most likely and common basis for people to process and store video material obtained from the dash-cams are legitimate interests pursued by the controller or by a third party according to the GDPR art 6 (1) (f).

3.1.1 Legitimate interest as a legal ground for data processing

When defining the legal grounds for processing personal data, two options arise: consent and legitimate interests. Generally, the legitimate interest of the controller may be overridden by the interests of individuals, meaning that if a recording intrudes on a data subject’s privacy, it will most likely require consent of the recorded individual. It is practically impossible to gather a recorded person’s consent, therefore it is only possible to use dash cams on the basis of legitimate interest. Unlike consent, using legitimate interest of the driver as a basis for data processing is a feasible way to gather data, e.g. for gathering evidence and route monitoring.\textsuperscript{23}

The question arises whether using a dashcam camera during driving serves a legitimate interest pursued by the processor (dashcam user), which is not overridden by the interests or fundamental rights and freedoms of the data subjects (pedestrians and other people in traffic).

\textsuperscript{21} Handbook on European data protection law, p 151.
\textsuperscript{22} Handbook on European data protection law, p 152, General Data Protection Regulation, Recital 46.
The European Court of Justice has confirmed that there are 3 main criteria for the data to be processed on the basis of legitimate interests pursued by the controller. In the case no C-708/18 p 40, the court stated that Article 7(f) of Directive 95/46 (now repealed by General Data Protection Regulation) lays down three cumulative conditions in order for the processing of personal data to be lawful, namely:

1) first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed;

2) secondly, the need to process personal data for the purposes of the legitimate interests pursued;

3) thirdly, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued.24

The court has also brought out the same conditions in the case C-13/16 Rīgas satiksme.25

The European Court of Justice has discussed the legitimate interest exception in a case C-131/12. In the judgement the Court stated that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’. In the light of the potential seriousness of the interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in the processing. Whilst it is true that the data subject’s rights protected by those articles also override, as a general rule, the interests of internet users, the balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having the information, an interest which may vary, in particular, according to the role played by the data subject in public life.26

When taking into account the principles brought out in this judgement, it can be said that using this type of data (video recordings from dashcams) for developing a better product (dashcam or

24 Case C-708/18. TK v Asociaţia de Proprietari bloc M5A-ScaraA, Judgment of the Court.
smartphone app) is not possible, since the process lacks data subjects’ consent and it pursues merely the economic interest of the dashcam or smartphone app developers.

In Germany, there has been a court case regarding a situation, where two cars collided in traffic, causing minor material damage. One of the parties tried to use video of the crash recorded by a dashcam to prove that the other party was responsible for the crash. In the final instance the Bundesgerichtshof (BGH-The Federal Court of Justice) ruled that the recording violated data protection law, but the result of it (the video) may still be used as evidence in the court proceedings. The BGH first stated that the recording of the traffic by the Dashcam was the processing of personal data by the applicant, since it also provided information on recognizable license plates. BGH also mentioned that according to the CJEU Ryneš case, video recording on a continuous storage device, which extends to the public space is categorized as automated processing of personal data. BGH was of the position that the permanent and indiscriminate recording of road traffic violates data protection law.

In the same judgement, the court also described the principle of weighing interests. According to the court, the right to data protection of affected persons must also be taken into account, however, the applicant's interests are more important. The Court mentions two interests: general interests of the public - the interest in an effective administration of justice and the goal of arriving at a correct decision - as well as interests of the individual, in the specific case in the form of the interests of the evidence in the enforcement of his civil rights claims. The Court interestingly also brings out, that there is no similarity between the secret recording of the spoken word and the video shots that were taken in public transport areas, where people are exposed to observation of other road users.

29 C. Etteldorf, About Dashcams und Digital Estate. P 373.
3.2 Drivers as Controllers of the Dash Cam video data

The controllers of the Dash cam video are usually the drivers who own the camera or in a fleet setups, the companies operating the fleet. It is also possible that there are multiple controllers, for example when an insurer offers the incentive to a policyholder of installing a dash cam in his or her vehicle in an attempt to reduce fraudulent injury claims, both the insurer and the relevant policyholder become data controllers. This was confirmed by the Irish Data Protection Commission, which also stated that such a scenario requires the parties to enter into a joint controllership agreement. This type of agreement establishes the distribution of responsibility between the two controllers - they are often complex and take time to negotiate. However, in an insurance setup, it is difficult to envisage how this could work on a large scale unless through the use of pre-completed forms and nonnegotiable terms. The main obligations for controllers regarding the use of dash cam use are: a) defining the lawful basis for collecting and using the data; b) keeping personal data secure and only for a definite period of time; c) handling personal data in a transparent manner; d) being able to provide a copy of a recording.

3.3 Legal grounds for sharing the recordings

Those using a dash cam in a public area for security or accident liability purposes should be aware that the publication of footage, for example on social media platforms, could represent a further act of processing and could risk infringing the data protection rights of recorded individuals. In general, and in line with the CJEU’s reasoning in the Buivids case (C–345/17), publication of material to an indefinite audience, such as on a fully public social media channel, cannot be considered to fall within the personal or household exemption. For any use of recordings involving personal data, which do not fall within an exception to data protection law, the controller will need to ensure that they have a legal basis for doing so, and otherwise meet the principles of data protection. Publication of personal data can be justified in certain circumstances for journalistic purposes, but this must be carefully balanced with the data protection rights of the individuals concerned.

---

The most controversial coverage in the news of dash cam recordings has been brought on by YouTube publications of traffic violations and reckless behavior. Even though this may seem like a way to generate likes, webpage controllers should make sure that drivers are banned from any such sharing because of the high risk of violating privacy laws. This is also true in individual cases.\textsuperscript{34}

Anna Rak-Kozerska, a recognized privacy attorney, has said that this may be solved by redaction. For example, in Germany, recordings may be shared if personal data is blurred. In very specific circumstances, publication of a video recording may be justified by journalistic purposes, but such purposes are generally unlikely if someone is using a dash cam for security or accident liability evidence. Thus, even in such a case, there is a large body of case law which governs the relationship between freedom of speech and an individual’s right to privacy as protected by Article 8 of the European Convention on Human Rights.\textsuperscript{35}

In some cases, public authorities or enforcement agencies may request access to recordings. Public authorities should be able to demonstrate that the recording is necessary for the purposes of an investigation or prosecution of a criminal offence, otherwise the controllers of dash cam videos should not disclose the footage. According to the Estonian Personal Data Protection Act § 12 (3) second sentence, GDPR shall not apply to law enforcement authorities, unless otherwise provided for in this Act.\textsuperscript{36}

Tallinn Circuit Court has discussed the use of dash cam recording as evidence in misdemeanor proceedings. In the proceedings, a person (J.H.) caused a dangerous situation in traffic and stopped the car in the middle of the road, exited the car, took a baseball bat and threatened the person who was sitting in a car behind the stopped car. The person, who threatened another person with the baseball bat, was caught on the dashcam recording of the victim. J.H. later claimed that the recording could not be used in the proceedings since he had not given permission to be filmed during the incident. The Harju County court disagreed with J.H. that the video recording was not

\textsuperscript{34} A.Rak-Kozerska, How to use dashboard cameras in a compliant way - Accessible: https://www.wsgr.com/PDFSearch/dashboard-cameras.pdf (01.01.2020)

\textsuperscript{35} A.Rak-Kozerska, How to use dashboard cameras in a compliant way - Accessible: https://www.wsgr.com/PDFSearch/dashboard-cameras.pdf (01.01.2020)

\textsuperscript{36} Personal Data Protection Act.- RT I, 04.01.2019, 11.
admissible evidence. The County Court explained that according to VtMS § 2 and KrMS § 63 lg 1, a photo, film or other information on a storage medium can be considered to be evidence. According to the court, the on-board camera recording of a motor vehicle is admissible evidence - pursuant to IKS § 14 lg 2 p 1 the communication of personal data for the purposes of processing is permitted without the consent of the data subject, if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law. According to the County Court, the transmission of the on-board camera recording to the police for carrying out either criminal proceedings or misdemeanor proceedings is therefore lawful without the consent of the data subject. The county court also referred to the Supreme Court judgement no 3-1-1-33-11, where it was stated that the recording of a private telephone conversation, for example, is admissible evidence and that it was not collected in violation of the requirements of the KrMS § 64.37

Drivers are allowed to use recordings as evidence in the context of preventive recording, but the driver should ensure that the one who is receiving the evidence, has appropriate data processing and retention policies in place.38

Whether a dash cam video filming and processing needs to comply with the GDPR will need to be assessed on a case-by-case basis. This was affirmed in the Ryneš case (C-212/13, December 2014), in which the European Court of Justice concluded that where a surveillance camera on a private domestic property is fixed in a way that it monitors a public space, the recording cannot be considered as made only for domestic use. According to the case, during the period from October 2007 to April 2008, Mr Ryneš installed and used a camera system located under the eaves of his family home which was installed in a fixed position and could not turn. It recorded the entrance to his home, the public footpath and the entrance to the house opposite. The recording was later relied on in the course of the subsequent criminal proceedings where two individuals had broken Mr Ryneš’ house windows. A request from one of the suspects was made to question the legality of the recording since there was no consent by the criminal to film him.39

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is no longer in force as it was repealed by the General Data Protection Regulation.\textsuperscript{40}

According to EU court case p 21 and 11, the term ‘personal data,’ as used in that provision, covers, according to the definition under Article 2(a) of Directive 95/46, ‘any information relating to an identified or identifiable natural person’, an identifiable person being ‘one who can be identified, directly or indirectly, in particular by reference … to one or more factors specific to his physical … identity’. Accordingly, the image of a person recorded by a camera constitutes personal data within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned.\textsuperscript{41}

According to p 34, at the same time, the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings.\textsuperscript{42}

In the light of the decision C-212/13, the court confirmed that the protection of the property, health and life of persons can be considered as legitimate interests pursued by the controller according to the Article 7(f) of the Directive 95/46 (now repealed by GDPR art 6 (1) (f)).

3.4 Processing special category data

Problems arise, when special category data is being recorded with dashcams or smartphones. According to the GDPR art 9, special category data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

\textsuperscript{41} C-212/13, December 2014. European Court of Justice.
\textsuperscript{42} C-212/13, December 2014. European Court of Justice, p. 34.
genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.43

Article 9 (2) (e) of the GDPR provides that processing is not prohibited if it relates to data which are manifestly made public by the data subject. Thus, where the television broadcasts a video taken from a video surveillance camera, showing, among other things, a firefighter getting injured trying to evacuate a building, it cannot be considered that the firefighter has manifestly made public the data. On the other hand, if the firefighter decides to describe the incident and publish the video and photos on a public internet page, he or she would have made a deliberate, affirmative act to make the personal data public. It is important to note that making one’s data public does not constitute consent, but it is another permission for processing special categories of data.44

It can therefore be said that if a car accident is filmed with a dashcam, the video surveillance of the person getting injured constitutes data concerning health, which are special category data. This type of data may only be processed, according to the rules set forth in the GDPR art (9)(2). If the person has not manifestly made public by the video of the car accident, but it is somehow leaked, it cannot be considered that the accident victim has manifestly made public the data.

The same applies to public displays of affection, e.g. a couple holding hands or kissing, which may reveal data regarding the persons’ sexual orientation. Public displays of affection may not be equated to making the persons’ sexual orientation manifestly public, as it is possible they are not aware of being filmed.


44 2018 GDPR handbook. pg 162.
4 SOLUTIONS ON HOW TO COLLECT TRAFFIC VIDEO DATA IN COMPLIANCE WITH GDPR

Dash cams are becoming more and more popular in many parts of the world, including Europe. Drivers are using dash cams to protect themselves in case of traffic accidents so as to provide proof of their innocence. The same applies to traffic cameras, ADAS systems and smartphones - they are used for protection. What controllers of the video gathering methods usually do not know is that they have to process data in compliance with the GDPR, because all existing types of dashcams, smartphones, ADAS systems and other recording devices may accidentally capture personal information.

One approach to make dashcam recordings compliant with data protection law is to automatically identify personal information – at least pedestrian’s faces and license plates etc – in the captured video image and subsequently disguise them. The main information that have to be protected are faces and license plates. Furthermore, recording devices also produce metadata like timestamps and GPS locations, which may be embedded into the original video files or stored in separate files - this information has to be protected as well. These kinds of anonymization methods do exist already, but they are not being used in dash cams and smartphones because such methods are expensive to implement. The method works by anonymizing encrypted dashcam videos on a dedicated computer system before the user gets access to the videos. To accomplish this, classified images are safeguarded by usage control techniques on the way from the camera to the anonymization component. By applying this system, any existing dashcam can ultimately be enhanced by privacy protection capabilities.45

This declassification system ensures confidentiality and integrity of privacy by omitting relevant image areas in video data recorded by a dashcam and other recording devices. By outsourcing the anonymization to a separate computer system, it is possible to apply more powerful image processing algorithms so that the processing of personal information can be minimized according to the state-of-the-art, and any customary dashcam along with an encryption device can be

enhanced with privacy protection capabilities. Dash Cam, smartphone and ADAS system operation according to data protection requirements thus seems possible.

Another possible solution for dash cam footage to be compliant with General Data Protection Regulation would be incident recording, meaning that the camera will start recording right before the accident. It will be initiated by sudden braking or losing control of the car or driving too fast/slow. This would ensure that there is a valid reason for recording the incident and drivers are not collecting information that they should not have.

The BGH (The German Federal Court of Justice) also stated that the large amount of data (recording of traffic permanently from the dashboard) is not required for evidence or accident reconstruction, but only a small part of this data is needed. Therefore, it is possible to design special solutions and designs, which would limit the recording to a short-term event related storage—when accident is about to happen, motion sensors trigger the recording of the collisions and automated extinguishing mechanisms are used that delete obscure personal data.

According to some legal scholars, the most realistic and effective way of protecting subsets of privacy is threatening legal responsibility for breaches of people's privacy and clear and effective rules of the usage of image capturing devices. The advantages of new technologies should not be denied, therefore it would be absurd to assert that they may not be used, because they cause too much danger to data subjects’ privacy. Privacy as a right is absolute. It is essential to adapt legal mechanisms to the changing technological environment. Thus, the lack of legal measures could not be the reason to interfere with technological development: not that new technologies should be treated as a threat, but legal norms should be improved and adjusted to the constantly changing world.

47 C. Etteldorf, About Dashcams und Digital Estate. P 373.
CONCLUSION

Dash cams are becoming more and more popular in many parts of the world, including Europe. Not all the footage they collect are subject to General Data Protection Regulation. If the footage is kept for the collector and not published, then the household exemption applies and there is no need for compliance with the General Data Protection Regulation.49

The most likely and common basis for people to process and store video material obtained from the dash-cams are legitimate interests pursued by the controller or by a third party according to the GDPR art 6 (1) (f).

The European Court of Justice has confirmed that there are 3 main criteria for the data to be processed on the basis of legitimate interests pursued by the controller: the pursuit of a legitimate interest by the data controller to whom the data are disclosed, the need to process personal data for the purposes of the legitimate interests pursued and the fundamental rights and freedoms of the person concerned by the data protection must not take precedence over the legitimate interest pursued.50

The German Federal Court (BGH) brought out that the applicant's interests (person who uses dashcam footage as evidence) are more important than the data subjects’ interests. The Court mentions two interests: general interests of the public - the interest in an effective administration of justice and the goal aiming of arriving at a finding a correct decision - as well as interests of the individual, in the specific case in the form of the interests of the evidence in the enforcement of his civil rights claims.51

Tallinn Circuit Court has discussed the use of dash cam recording as evidence in misdemeanor proceedings. According to the court, the on-board camera recording of a motor vehicle is admissible evidence - pursuant to IKS § 14 lg 2 p 1 the communication of personal data for the

49 P. Aurelija, 2019.
50 Case C-708/18. TK v Asociaţia de Proprietari bloc M5A-ScaraA, Judgment of the Court.
purposes of processing is permitted without the consent of the data subject, if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law. According to the County Court, the transmission of the on-board camera recording to the police for carrying out either criminal proceedings or misdemeanor proceedings is therefore lawful without the consent of the data subject.52

One approach to make dash cam recordings compliant with data protection law is to automatically identify personal information – pedestrian’s faces and license plates etc. – in the captured video image and subsequently disguise them.53

Another possible solution for dash cam footage to be compliant with General Data Protection Regulation, could be incident recording, meaning that the camera will start recording right before the accident. It could be initiated by sudden braking or losing control of the car or driving too fast/slow.54

According to some legal scholars, the most realistic and the most effective way of protecting subsets of privacy is threatening legal responsibility for breaches of people's privacy and clear and effective rules of the usage of image capturing devices. It is essential to adapt legal mechanisms to the changing technological environment.55

REFERENCE LIST

27


27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
