Information and Data Protection Commissioner

CDP/COMP/891/2023

[redacted]

vs

[redacted]

COMPLAINT

1. By means of a letter dated the 9th October 2023, Mr [redacted] (the **"complainant"**) lodged a complaint with the Information and Data Protection Commissioner (the "**Commissioner**") in terms of article 77(1) of the General Data Protection Regulation[1] (the **"Regulation"**), alleging that the video devices[2] installed by Mr [redacted] (the **"controller"**) are capturing beyond his private property, and therefore, the complainant considered the processing of his personal data to be an infringement of the Regulation.

INVESTIGATION

2. Pursuant to the internal investigation procedure and article 58(1)(e) of the Regulation, by means of a letter dated the 25th October 2023, the Commissioner provided the controller with a copy of the complaint and requested the controller to submit any information which he deemed relevant and necessary to defend himself against the allegation raised by the complainant. In particular, the Commissioner requested the controller to submit copies of the image grabs taken from the footage of the video devices.

[1] 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).
[2] The device is installed on the property [redacted]

[redacted]

3. By means of a letter dated the 20th November 2023, the controller through his legal counsel, submitted the following arguments:

   a. that "[i]*n line with the concerns raised by Mr* [redacted]*'s legal counsel, my client had to file an official police report and a criminal complaint against Mr.* [redacted]*. This action was necessitated by video footage showing Mr.* [redacted] *deliberately damaging my client's vehicle. For your reference, please find a copy of the redacted Police report and the relevant Criminal Complaint*"[3];

   b. that the "*CCTV system was installed as a direct response to previous incidents where my client's vehicle suffered damage on two separate occasions. This measure was taken to ensure the safety and security of my client's property*";

   c. that "[i]*t is pertinent to note that in civil proceedings, liability cannot be established without conclusive proof identifying the perpetrator of a crime. This standard is even more stringent in criminal proceedings, where the burden of proof is beyond a reasonable doubt*";

   d. that the "*retention of CCTV footage, please find my client's justification in line with the General Data Protection Regulation (GDPR).*

      In compliance with the GDPR, specifically under the principles set out in Article 5 and the lawful basis for processing under Article 6, the use of CCTV at my client's property is justified on the following grounds:

      Legitimate interest *(Article 6(1)(f) GDPR): The primary purpose of installing CCTV cameras was to protect my client's property and ensure personal safety. Given the history of damage to the property, particularly the vehicle, there is a clear legitimate interest in monitoring and safeguarding the premises. Furthermore, the European Data Protection Board (EDPB) in its publication (Guidelines 3/2019 on processing of personal data through video devices), Version 2.0, Adopted on 29 January 2020 ... indicates that legitimate interest may be based on a real and hazardous situation, such as the purpose to protect property against burglary, theft or vandalism can constitute*

[3] A copy of the police report dated the 23rd September 2023 was submitted.

a legitimate interest for video surveillance. Furthermore, it states that the legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative). Which my client has amply outlined with the attached documents. It must be outlined that in this case, the surveillance of my client's property is not sufficient, and the European Data Protection Board (EDPB) in its guidelines accepted surveillance beyond one's property (Paragraph 27).

***Proportionality and Necessity**: The deployment of CCTV cameras is a proportionate response to the specific risks faced by my client. The installation was a necessary measure following previous incidents of vandalism and damage, and it is tailored to monitor areas that are particularly vulnerable to such incidents.*

***Data Minimisation** (Article 5(1)(c) GDPR): The CCTV system is configured to ensure that only a limited perimeter of property is under surveillance, thereby minimizing the capture of third-party data. This approach is in line with the principle of data minimization, ensuring that no more personal data is processed than is necessary.*

***Security of Processing** (Article 32 GDPR): Appropriate technical and organizational measures have been implemented to ensure the security of the data captured by the CCTV cameras, in compliance with Article 32 of the GDPR. This includes restricted access to the footage, secure storage, and regular reviews of the necessity of the data retention.*

***Transparency** (Article 5(1)(a) GDPR): My client has taken steps to ensure transparency in the use of CCTV, including clear signage indicating the presence of CCTV cameras, thereby informing visitors and passerby of the processing of personal data through video surveillance.*

***Compliance with Local Regulations:** The installation and operation of the CCTV system are in accordance with local laws and regulations governing surveillance and privacy."*

[redacted]

LEGAL ANALYSIS AND DECISION

4. In principle, the Commissioner recognises the need for the installation of a video device to ensure the security and safety of private property. However, appropriate and sufficient guarantees should be effectively provided to ensure that such device is not capturing a public space and, or third-party properties.

5. In this regard, it should be pointed out that article 1 and recital 10 of the Regulation aim to ensure a high level of protection of the rights and fundamental freedoms of natural persons, in particular, article 8 of the Charter of Fundamental Rights of the European Union, which states that each and every person has the right to the protection of their personal data.

6. Having noted the letter dated the 20th November 2023, wherein the controller submitted copies of the image grabs taken from the footage of the video devices, which demonstrate that the video devices are excessively capturing public space, including third party properties. As a result, this is leading to the collection and retention of the data of all the individuals accessing the monitored area, and thus, this constitutes a processing activity in terms of article 4(2) of the Regulation.

7. The Court of Justice of the European Union in the Ryneš[4] judgment held that video surveillance which "*covers, even partially, a public space and is accordingly directed outwards from the private setting of the personal processing the data in that manner, **it cannot be regarded as an activity which is a purely 'personal or household' activity***" [emphasis has been added]. This reasoning was endorsed by the Information and Data Protection Appeals Tribunal in relation to the decision '*Raymond u Mary Ann konjuġi Cutajar vs Kummissarju għall-Informazzjoni u l-Protezzjoni tad-Data*'[5], where a video device was installed on the façade of a private property in such a manner to capture public space.

8. In the present case, it is abundantly clear that the processing activity conducted by means of the CCTV does not fall within the household exemption in terms of article 2(2)(c) of the Regulation, and therefore, the processing of personal data should fully comply with the provisions of the Regulation and the rights and freedoms of the affected data subjects.

[4] Case C-212/13, paragraph 33.
[5] Appeal Number 4/2019, decided on the 27th October 2020.

9. The principle of lawful processing, which is one of the principles of data protection, states that every processing data operation needs to have a legal basis for processing. Therefore, article 6(1) of the Regulation stipulates what could constitute as a legal basis while also considering the other principles for data processing as stipulated in article 5 of the Regulation.

10. The European Data Protection Board[6] provides that every legal basis that falls under article 6(1) of the Regulation could provide a basis for the processing of personal data by means of video recording. The installation of the video device by private individuals which is capturing a public space is generally deemed to be unlawful, unless in very exceptional cases, the controller manages to concretely prove that there is a compelling legitimate interest to conduct this processing operation. However, even in such cases, the controller should strictly monitor the immediate surroundings of the property and not extensively monitor a public space and third-party properties. In fact, the EDPB states that "[i]*n some individual cases it might be necessary to exceed the video surveillance to* ***the immediate surroundings*** *of the premises*"[7]. In the present case, it is evident that the video devices are not merely capturing the immediate surroundings of the controller's property but are excessively monitoring public space and third-party properties.

11. In the submissions provided during the course of the investigation, the controller stated that the purpose of the processing is to prevent any damage to his vehicle. However, the Commissioner noted that the controller is monitoring a considerable area on the assumption that he will be able to find, on a daily basis, to park his vehicle and have it monitored. In the light of the fact that the controller does not have an exclusive reserved parking sport nor a divine right to park his vehicle in one of the available parking spaces which are captured within the angle of view of these video devices, the Commissioner established that the processing is excessive, and is leading to the processing of personal data of all the individuals accessing the monitored area.

12. After assessing the submissions provided by the controller, the Commissioner concluded that the controller had not managed to effectively demonstrate that there is indeed a lawful basis that could legitimise the processing activity conducted by means of the video devices. The systematic and continuous monitoring of a public space and third-party properties, which leads

[6] Guidelines 3/2019 on Processing of Personal Data through Video Devices, Version 2.0, adopted on the 29th January 2020, paragraph 16.
[7] Ibid. 6, para. 27.

to the processing of personal data of all the data subjects in a general and non-discriminate manner, is deemed to be unlawful and an infringement of the rights and freedoms of the data subjects.

In the light of the foregoing considerations, the Commissioner hereby decides that the processing activity undertaken by the controller by means of the video devices is not in conformity with article 6(1) of the Regulation.

By virtue of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to adjust the angle of view of the video devices in such a manner to solely capture his private property. If this is not possible due to a technical reason or any other reason whatsoever, the video devices shall be removed. The controller shall comply with this order by no later than twenty (20) days from the date of receipt of this legally binding decision.

The controller is requested to inform the Commissioner of the corrective action taken immediately thereafter, supported by copies of the image grabs or photographic evidence that the devices have been removed. The information about the action taken shall be submitted by means of an email on idpc.cctv@idpc.org.mt

In terms of article 83(6) of the Regulation, "[*n*]*on compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to an administrative fine up to 20 000 000 EUR*".

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

The parties are hereby being informed that in terms of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal to the Information and Data Protection Appeals Tribunal within twenty (20) days from the service of the said decision as provided in article 23 thereof.

An appeal to the Tribunal shall be made in writing and addressed to "The Secretary, Information and Data Protection Appeals Tribunal, 158, Merchants Street, Valletta."