

██████████

vs

██

COMPLAINT

1. On the 30th October 2025, ██████████ (the “**complainant**”) lodged a data protection complaint with the Information and Data Protection Commissioner (the “**Commissioner**”) in terms of article 77(1) of the General Data Protection Regulation¹ (the “**Regulation**”), alleging that ██████████ (the “**controller**”) installed CCTV cameras in the canteen area of its ██████████, unlawfully capturing himself and other employees during their break and rest time.
2. The complainant submitted that “[s]uch surveillance is excessive and not justified by legitimate security needs. The canteen is intended as a rest area, and employees do not feel comfortable taking their breaks while their personal data is being captured through CCTV cameras. Furthermore, the employer has indicated that footage from these cameras is being used for disciplinary purposes”. As supporting evidence, the complainant submitted a letter addressed to him, dated the 17th September 2025, in which he was accused of gross misconduct for consuming wine during his break time, allegedly reported and verified through CCTV camera recordings by the controller’s human resources department.

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).

INVESTIGATION

Request for submissions

3. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complaint, including the supporting document, and enabled the controller to submit any arguments and information that it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

Submissions of the controller

4. By means of an email sent on the 12th December 2025, the controller submitted (i) a copy of its communication with this Office concerning Data Protection Impact Assessments, (ii) a copy of the Article 29 Data Protection Working Party's *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* ("**Article 29 Working Party Guidelines**"), and (iii) a letter containing the following arguments for the Commissioner to consider during the legal analysis of the case:
 - a. that the CCTV camera in the canteen is clearly visible, appropriate signage is displayed, and all employees are informed about the CCTV system during onboarding and required to acknowledge this by signing a consent form;
 - b. that the "*the primary legal justification for CCTV in the workforce is not consent but legitimate interest*";
 - c. that the installation of CCTV in the canteen is justified by documented patterns of interpersonal incidents among employees, including "*physical altercations, bullying, inappropriate conduct, sexual harassment and other behaviour which poses risks to employee wellbeing. There have also been instances involving alcohol consumption, such as in this case, which is strictly prohibited due to the hazardous nature of the work environment*";
 - d. that the installation of CCTV in the canteen is considered necessary to ensure "*the safety and protection of all employees, safeguard company property and have the ability to investigate the lengthy variety of incidents*", rather than to monitor employees' behaviour during breaks;

- e. that the CCTV camera in the canteen is considered necessary and proportionate “*for the purposes of preventing and addressing misconduct, ensuring a safe working environment, and protecting both the company’s and the employees’ legitimate interests*”;
- f. that the CCTV footage is not monitored in real time but is accessed only in response to reported or suspected incidents;
- g. that in this case, a separate investigation led to the review of the canteen CCTV footage, which revealed alcohol consumption by the complainant;
- h. that following an assessment of whether a Data Protection Impact Assessment (“**DPIA**”) was required for the installation of such a CCTV camera, taking into account the Article 29 Working Party Guidelines, and following communication with this Office, it was concluded that no DPIA was necessary, as the conditions set out in Article 35(3)(c) of the Regulation were not met;
- i. that the controller took the necessary steps to ensure that the CCTV system complies with applicable data protection legislation, including by providing clear information to employees about the CCTV cameras on the controller’s sites, implementing a limited retention period, ensuring restricted access to footage, using the system exclusively for security, safety and incident-related purposes, and ensuring that the surveillance is proportionate to the organisation’s legitimate needs;
- j. that “*in evaluating the proportionality and necessity of this measure, the broader context of the [REDACTED] operational environment must be given meaningful weight. The realities we are required to manage are not hypothetical [...] It is within this concrete and documented context – not in abstraction – that the canteen CCTV must be assessed. The canteen is the primary congregation point for workers and therefore the location where many of these incidents could happen. Surveillance in this area is therefore not an excessive intrusion, nor is it aimed at monitoring employees during their breaks. It is a targeted, proportionate and objectively justified measure to prevent, deter and properly investigate misconduct that could place employees or the organisation at risk*”; and

- k. that the complaint seems to have arisen only after the CCTV footage was used against the complainant in disciplinary proceedings, suggesting that the surveillance itself was not previously disputed and thereby undermining the credibility of the complaint.
5. Following a review of the controller's submissions, the Commissioner, in terms of article 58(1)(a) of the Regulation, requested the controller to provide the following information:
 - a. evidence of the CCTV camera signage that is displayed;
 - b. evidence and information on how the employees are informed about the CCTV system during onboarding; and
 - c. evidence substantiating the submission made that the installation of the CCTV camera is required in view of a "*concrete and documented context*", namely a "*persistent pattern of interpersonal conflicts, physical altercations, bullying, harassment, misconduct among other*".
6. By means of an email sent on the 6th January 2026, the controller submitted the following documentation:
 - a. two photos showing CCTV camera signage outside and inside the canteen;
 - b. a copy of the acknowledgement signed by the complainant, confirming receipt of the controller's Employee Privacy Notice and CCTV Policy, and that he has read and understood them in their entirety; and
 - c. a four-page document containing a table with four columns, namely: (i) type of misconduct (minor/gross), (ii) "██████" reference, (iii) employer, and (iv) reason for the investigation. The table lists thirty-one (31) cases of gross misconducts, of which five (5) include "██████" (the name of the controller's site relevant in this case) in the "██████" reference.
7. Following a review of the documentation submitted by the controller, the Commissioner, in terms of article 58(1)(e) of the Regulation, requested the controller to provide the following further information:
 - a. information and, if available, evidence of when the CCTV camera signs were affixed;
 - b. a copy of the controller's Employee Privacy Notice and CCTV Policy;

Moreover, since according to the controller's submissions, the legal basis relied upon in this case is legitimate interest (Article 6(1)(f) of the Regulation), the Commissioner further requested the controller to provide the legitimate interest assessment ("**LIA**") carried out to justify such processing of personal data.

8. By means of an email sent on the 27th January 2026, the controller informed that it does not hold any records or evidence indicating when the CCTV signage in the canteen was affixed, noting that such documentation was not considered necessary at the time. However, based on internal staff confirmations, the controller maintains that the signs were in place prior to the incident, although the exact date remains unknown. Moreover, the controller provided a copy of the CCTV Policy “ [REDACTED] ” and a blank acknowledgment form confirming receipt, reading, and understanding of the Employee Privacy Notice and CCTV Policy. The LIA was neither submitted nor referred to in the controller’s email of 27th January 2026.

9. By means of another email sent on the same day, the 27th January 2026, the controller submitted the following further documentation:
 - a. the Data Protection Privacy Notice “ [REDACTED] ”;
 - b. the Health Data Privacy Notice “ [REDACTED] ”; and
 - c. a blank Data Privacy Notice form.

10. Following a review of the further documentation submitted by the controller, the Commissioner, in terms of article 58(1)(e) of the Regulation, requested the controller to provide the following further information and clarifications:
 - a. confirmation of the number of CCTV cameras installed in the canteen;
 - b. photos showing the CCTV camera(s) installed in the canteen;
 - c. a copy of the image grab taken from the footage of the CCTV camera(s) installed in the canteen;
 - d. the brand and model number of the CCTV camera(s) installed in the canteen; and
 - e. confirmation as to whether an LIA was conducted in relation to the CCTV camera(s) installed in the canteen.

11. By means of an email sent on the 9th February 2026, the controller submitted the following information and documentation:
 - a. confirmation that only one (1) CCTV camera is installed in the canteen;
 - b. one (1) photograph showing the CCTV camera installed in the canteen;
 - c. a copy of the image grab taken from the footage of the canteen CCTV camera;
 - d. the brand and model number of the canteen CCTV camera; and
 - e. confirmation that no LIA was concluded in relation to the CCTV camera in the canteen.

Submissions of the complainant

12. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the complainant with a copy of the controller's submissions sent on the 12th December 2025, as well as the supporting documentation submitted on the 6th and 27th January 2026, and enabled the complainant to rebut the controller's submissions. By means of an email sent on the 16th February 2026, the complainant submitted the following arguments:

- a. that the CCTV camera is installed in an employee rest area where a higher expectation of privacy applies, yet the controller relies only on general examples of workplace misconduct but provides no evidence that such incidents occurred in the canteen or that this specific area poses a risk warranting continuous monitoring. Consequently, the measure does not satisfy the requirements of necessity and proportionality under the Regulation;
- b. that although the controller claims that footage is accessed only when incidents arise, its CCTV Policy expressly allows use for employee performance monitoring and disciplinary proceedings, indicating a broader employee oversight function beyond security. In this context, the systematic monitoring of employees, who are recognised as vulnerable data subjects due to the imbalance of power, heightens the risk to their rights and freedoms;
- c. that the use of CCTV footage, initially reviewed for a separate matter, to identify unrelated misconduct indicates function creep and broader behavioural monitoring beyond the investigation of specific security incidents, raising concerns under the Regulation's purpose limitation principle;
- d. that the CCTV policy receipt acknowledgement predates the installation of the camera in the canteen, meaning employees were not specifically informed that this rest area would be subject to continuous monitoring. This expansion in surveillance without clear, prior notice raises concerns regarding compliance with the Regulation's transparency and fairness principles;
- e. that the continuous workplace monitoring of employees, who are a vulnerable group subject to a power imbalance, and potential behavioural assessment, likely entails high

risk to their rights and freedoms. The absence of a DPIA therefore raises concerns regarding compliance with Article 35 of the Regulation;

- f. that less intrusive alternatives exist to ensure employees' safety and safeguard the controller's property, and that employee monitoring in a non-operational rest area should be a measure of last resort, rendering the current measure disproportionate; and
- g. that the use of CCTV in the canteen is thus excessive and not strictly necessary, raising concerns regarding necessity, proportionality, transparency, purpose limitation, and accountability under the Regulation.

Final submissions of the controller

13. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complainant's rebuttal and enabled the controller to submit its final submissions. By means of an email sent on the 11th March 2026, the controller submitted the following concluding counterarguments:

- a. that while the complainant attempts to frame the CCTV installation within the canteen as excessive and unlawful, the arguments advanced rely on selective interpretation of the Regulation's principles and mischaracterisations of the facts and the applicable legal framework;
- b. that the specific location of the camera is not determinative of the lawfulness of the processing. The examples of misconduct provided by the controller show that misconduct is not limited to operational areas but can occur wherever employees gather, including the canteen, which is the primary communal area within the facility and "*one of the most likely locations where interpersonal incidents may arise*". A reactive approach by installing CCTV only after incidents occur would undermine preventive workplace safety and expose both employees and the organisation to unnecessary risks. Installing CCTV in a shared rest area therefore serves the legitimate purposes of deterring misconduct and providing objective evidence when incidents arise;
- c. that the complainant's claim of "*systematic monitoring*" is unfounded since the CCTV system is passive, not continuously or methodically observed, and footage is accessed

only when an incident is reported or suspected. The complainant's argument wrongly equates the possibility of accessing recordings with the existence of a structured monitoring programme. Although recital 75 of the Regulation highlights risks linked to profiling or systematic evaluation, the canteen CCTV camera "*does not structurally analyse or evaluate employee performance, does not generate behavioural profiles, and is not used for continuous observation or monitoring of employees' activities*", and references to "*monitoring*" in the controller's CCTV policy simply mean the ability to view recordings when necessary, not continuous oversight or behavioural tracking;

- d. that the complainant's claim of "*function creep*" is unfounded because the CCTV system is not continuously monitored, and there is "*no active review of footage absent a triggering event*". The complainant's misconduct was in this case only discovered "*because the footage was reviewed in relation to a separate incident. Had that unrelated investigation not occurred, the conduct in question may never have been discovered*". This shows the system is not used for broader behavioural monitoring. Incidental discovery of misconduct during a legitimate investigation cannot be characterised as "*function creep*";
- e. that the complainant's argument that the transparency obligations under the Regulation were not met because the CCTV policy receipt acknowledgment predates the installation of the canteen CCTV camera does not take into account that the CCTV policy constitutes a general framework applicable to both existing and future installations and is not reissued each time a new camera is added. Employees were informed of the CCTV system through this policy and through clear on-site signage, which together are intended to meet the Regulation's transparency requirements; and
- f. that the complaint's allegation regarding the need for a DPIA is unfounded, for the reasons set out in the controller's initial submissions, namely that the criteria triggering a mandatory DPIA under Article 35(3)(c) of the Regulation are not met in this case.

LEGAL ANALYSIS AND DECISION

14. The Commissioner proceeded to examine the complaint lodged by the complainant, wherein he alleged that the controller had installed CCTV cameras in the canteen area of its [REDACTED], unlawfully capturing himself and other employees during their break and rest time in breach of the Regulation.

15. During the course of the investigation, in terms of article 58(1)(e) of the Regulation, the Commissioner requested the controller to clarify, *inter alia*, the number of CCTV cameras installed in the canteen area and to provide photographs of such CCTV cameras together with a copy of the image grab taken from their footage. The controller complied with the request of the Commissioner and submitted the requested information. Following an examination of such information, the Commissioner established that the controller had installed only one (1) CCTV camera in the canteen area, as evidenced by the controller's submissions sent on the 9th February 2026, including the photograph showing the CCTV camera installed in the canteen and the copy of the image grab taken from the footage of that camera.
16. For the purposes of this legal analysis, the Commissioner proceeded to assess whether the controller has a valid legal basis in terms of article 6(1) of the Regulation to process the personal data of the employees that enter the monitored area captured by the CCTV camera installed in the canteen of its [REDACTED].
17. In Guidelines 3/2019², the European Data Protection Board (the “EDPB”) states that “[i]n principle, every legal ground under Article 6(1) can provide a legal basis for processing video surveillance data. For example, Article 6(1)(c) applies where national law stipulates an obligation to carry out video surveillance. However, in practice, the provisions most likely to be used are article 6(1)(f) (legitimate interest) [and] article 6(1)(e) (necessity to perform a task carried out in the public interest or in the exercise of official authority. In rather exceptional cases Article 6(1)(a) (consent) might be used as a legal basis by the controller”.
18. The Commissioner assessed the controller's submissions and noted the following from the submissions sent on the 12th December 2025: “*All employees are also informed about the CCTV system during onboarding and our also given a consent form to be signed. **Although employee consent is collected, we emphasize that the primary legal justification for CCTV in the workforce is not consent but legitimate interest, as recognised under the GDPR. Thus, CCTV is implemented on the basis of legitimate interests pursued by the company and all employees are transparently informed about such surveillance***” [emphasis has been added].
19. The Commissioner further assessed the supporting documentation, in particular the complainant's signed acknowledgement confirming receipt and understanding of the controller's CCTV Policy, submitted by the controller on the 6th January 2026 in compliance

² Guidelines 3/2019 on processing of personal data through video devices, version 2.0, adopted on the 29th January 2020, paragraph 16.

with the Commissioner's request for additional information in terms of article 58(1)(a) of the Regulation. This document bears the complainant's signature confirming receipt of the controller's Employee Privacy Notice and CCTV Policy, and that he has read and understood them in their entirety. The Commissioner noted that, while this document does not constitute consent, it forms part of the controller's measures aimed at fulfilling its transparency and information obligations under the Regulation. In this regard, the Commissioner notes that consent under article 6(1)(a) of the Regulation, by its nature, is generally unsuitable as a legal basis in the employment context. As the EDPB states in Guidelines 3/2019, "[g]iven the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given"³, which in practice often leads controllers to consider alternative bases such as legitimate interests under article 6(1)(f) of the Regulation.

20. The Commissioner further noted section 8 entitled "*Legal Basis for Processing*" of the CCTV Policy "████████████████████" submitted by the controller on the 27th January 2026 in compliance with the Commissioner's request for additional information in terms of article 58(1)(e) of the Regulation, which provides as follows: "*The Company justifies the use of a CCTV system(s) for the above-mentioned purposes for its **legitimate business interests (Article 6 (1) (f) of the GDPR)**...*" [emphasis has been added].
21. In view of the foregoing considerations, the Commissioner established that the controller is basing its processing activity conducted by means of the CCTV camera in the canteen on article 6(1)(f) of the Regulation, which enables the controller to process personal data if it "*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*".
22. The Commissioner therefore proceeded to consider the applicability of article 6(1)(f) of the Regulation for the controller's processing activity conducted by means of the CCTV camera in the canteen.
23. Recital 47, which corresponds to article 6(1)(f) of the Regulation, specifies the content and scope of this legal basis for processing and stipulates that the "*legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, **provided that the interests or the***

³ Ibid., paragraph 47.

*fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate **the existence of a legitimate interest would need careful assessment...*** [emphasis has been added].

24. The Court of Justice of the European Union (the “CJEU”) has consistently held that the reliance on article 6(1)(f) of the Regulation as a legal basis for the processing of personal data is contingent on the satisfaction of a **three-part test**, which is outlined hereunder:

“According to settled case-law, that provision lays down three cumulative conditions so that the processing of personal data covered by that provision is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party (judgments of 4 July 2023, Meta Platforms and Others (General terms of use of a social network), C-252/21, EU:C:2023:537, paragraph 106, and of 4 October 2024, Koninklijke Nederlandse Lawn Tennisbond, C-621/22, EU:C:2024:857, paragraph 37)”⁴.

25. In this respect, the Commissioner examined the present case based on the three cumulative conditions established by article 6(1)(f) of the Regulation. These conditions are: (i) the existence of a legitimate interest justifying processing; (ii) the necessity of processing for the realisation of the legitimate interest; and (iii) the prevalence of that interest over the rights and interests of the data subject, which calls for balancing of interests.
26. Under the accountability principle laid down in article 5(2) of the Regulation, the controller is responsible for, and must be able to demonstrate, the lawfulness of the processing activity conducted by means of the CCTV camera in the canteen, including that the three (3) cumulative conditions set out above are fulfilled.

⁴ Case C-394/23 *Mousse v Commission nationale de l’informatique et des libertés (CNIL) and SNCF Connect* [2025] ECLI:EU:C:2025:2, paragraph 45.

27. During the course of the investigation, in terms of article 58(1)(e) of the Regulation, the Commissioner specifically requested the controller to provide the legitimate interest assessment (“LIA”) carried out to justify the processing activity conducted by means of the CCTV camera in the canteen under article 6(1)(f) of the Regulation. However, in its reply sent on the 27th January 2026, the controller made no reference to the LIA. Accordingly, the Commissioner again requested the controller to provide further information, including a confirmation as to whether an LIA had been conducted in relation to the CCTV camera in the canteen.
28. By means of an email sent on the 9th February 2026, the controller stated that “[n]o legitimate interest assessment was conducted in relation to the CCTV including a DPIA for the reasons explained in our reply. We maintain our position that the camera in question, considering the context in which it is being used, is a basic need for the company to safeguard its basic interests”.
29. The Commissioner remarks that an LIA and a DPIA are distinct exercises under the Regulation, although they may overlap in practice. An LIA is undertaken where a controller intends to rely on article 6(1)(f) of the Regulation as the lawful basis for processing. By contrast, a DPIA is not triggered by the legal basis relied upon, but by the risk profile of the processing, and serves to assess whether the envisaged processing is likely to result in a high risk to the rights and freedoms of natural persons, and to identify measures to mitigate such risks. In fact, in Guidelines 1/2024⁵ which analyse the criteria set down in article 6(1)(f) of the Regulation, the EDPB states that “if high risks are identified in the context of [the assessment of the abovementioned third condition], the controller should consider performing a Data Protection Impact Assessment (DPIA) in accordance with Article 35 GDPR”. The Commissioner further notes that, unlike a DPIA under article 35 of the Regulation, which is mandatory only where the conditions laid down therein are met, reliance on Article 6(1)(f) of the Regulation necessarily requires the controller, in every case, to assess and be able to demonstrate the existence of a legitimate interest pursued, the necessity of the processing for that purpose, and that such interest is not overridden by the rights and freedoms of the data subjects concerned. As explained by the EDPB in Guidelines 1/2024, this “assessment should be made at the outset of the processing, with the involvement of the Data Protection Officer (DPO) (if designated), and should be documented by the controller in line with the accountability principle set out in Article 5(2) GDPR”.⁶

⁵ Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, version 1.0, adopted on the 8th October 2024, paragraph 49.

⁶ Ibid., paragraph 12.

30. In the present case, the controller confirmed that no LIA was conducted in relation to the canteen CCTV camera. The Commissioner therefore proceeded to assess the three (3) cumulative conditions on the basis of the controller's submissions and supporting documentation, particularly its CCTV Policy sent by email on the 27th January 2026.
31. First, the processing is conditional upon the existence of a legitimate interest of the controller or a third party. The Regulation does not define "*legitimate interest*", and thus, it is for the controller to determine whether there is a legitimate aim that could justify an interference with the right to the protection of personal data. The Commissioner interprets "*interest*" to be the broader stake that a controller may have in the processing, or the benefit that the controller or third parties may derive from such processing. This interpretation is substantiated by the recitals of the Regulation, which provide some non-exhaustive examples of situations in which legitimate interest could exist, for example for the purpose of preventing fraud. Furthermore, the CJEU has acknowledged that the protection of the property, health and family life, could be legitimate interests.⁷ This position is reiterated by the EDPB in Guidelines 1/2024, which further explain that the interest must be lawful, clearly identified, and already present at the time of the processing.⁸
32. In its submissions sent on the 12th December 2025, the controller stated that the canteen CCTV camera is necessary for "*protecting both the company's and the employees' legitimate interests*". However, the controller's submissions do not specify the particular legitimate interests relied upon but section 8.1 of the controller's CCTV Policy provides as follows: "*The Company justifies the use of a CCTV system(s) for the above-mentioned purposes for its legitimate business interests (Article 6 (1) (f) of the GDPR) such as maintaining public safety, security of property and premises, prevention and investigation of crime, safety of staff, clients, suppliers and visitors and quality control. Furthermore, it is also within the employees' legitimate interest to monitor and consequently keep them safe and secure by preventing crime, preventing employee misconduct, ensuring compliance with health and safety procedures, monitoring and improving productivity, and comply with regulatory requirements.*" [emphasis has been added].
33. In this regard, while the protection of the controller's property, the prevention of misconduct, the safeguarding of workplace discipline and compliance with procedures may, in principle,

⁷ Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428 paragraph 34.

⁸ Guidelines 1/2024 (n 5) paragraphs 16-17.

constitute legitimate interests capable of being pursued under article 6(1)(f) of the Regulation, the Commissioner observes that the controller's reliance on the wording "*such as*" in its CCTV Policy is inconsistent with the requirement of specificity. In this respect, the Commissioner strongly urges the controller to adopt a well-defined CCTV Policy. Legitimate interests must be identified in a clear, specific, and precise manner. The scope of the interest pursued must be sufficiently defined so as to enable a proper assessment of necessity and an effective balancing exercise against the interests and fundamental rights and freedoms of the data subjects concerned.

34. As to the second condition relating to the necessity of the processing, the Commissioner assessed if the processing is "*strictly necessary*"⁹ for the purpose of the attainment of the legitimate interests at issue and whether such interests "*cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects*".¹⁰ The Commissioner noted that the principle of data minimisation as laid down in article 5(1)(c) of the Regulation requires that the processing must be adequate, relevant and limited to what is necessary in relation to the purpose of the processing. It therefore follows that the processing of personal data must be limited to what is plausibly necessary to pursue a legitimate interest and there must be a connection between the processing and the interest pursued.
35. During the course of the investigation, in terms of article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide, *inter alia*, evidence substantiating its submission that the installation of the CCTV camera was necessary in view of a "*concrete and documented context*", namely a "*persistent pattern of interpersonal conflicts, physical altercations, bullying, harassment, misconduct among other*". The controller complied with that request and, on the 6th January 2026, submitted a four-page document containing a table listing thirty-one (31) cases of misconduct. In his submissions, the complainant argued that the controller relied only on general examples of workplace misconduct without providing evidence that such incidents occurred in the canteen area or that this specific area posed a risk warranting continuous monitoring. In its final submissions, the controller argued that the footage of the CCTV camera is not continuously monitored, but that it is accessed only when an incident is reported or suspected. The controller further submitted that the examples of misconduct demonstrate that such behaviour is not limited to operational areas, but may occur wherever

⁹ Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537 paragraph 126.

¹⁰ *Ibid.*, paragraph 108; Guidelines 3/2019 (n 2) paragraph 24.

employees gather, including the canteen, which is “*one of the **most likely** locations where interpersonal incidents **may** arise*” [emphasis has been added].

36. The Commissioner acknowledges that accessing the CCTV footage only when an incident is reported or suspected is less intrusive than continuous live monitoring. The Commissioner further acknowledges that the controller implemented certain measures in pursuit of the data protection principles, including a limited retention period, appropriate CCTV signage, and restricted access to the footage. However, the Commissioner is not entirely satisfied that the processing activity conducted by means of the CCTV camera in the canteen area is strictly necessary for the pursuit of the legitimate interests invoked. The Commissioner notes that only five (5) of the thirty-one (31) cases of misconduct listed in the table provided by the controller relate to the site relevant in this case (“**██████████**”), and that the table does not specify the precise location of those incidents within that site. The table merely indicates that the five incidents concerned: “*Verbal Sexual Harassment / Violation of Company Policy*”, “*Major Insubordination*”, “*Disregarding Health & Safety Regulations / Sleeping during working hours*”, “*Disregarding Health and Safety Regulations / Consuming alcohol at work*”. In the Commissioner’s view, this table is insufficient to establish repeated serious misconduct in the relevant canteen area, particularly in light of the speculative wording of the controller’s final submission that the canteen is one of the “*most likely*” areas where incidents “*may*” occur. Moreover, the controller provided no evidence demonstrating that less intrusive measures than CCTV monitoring, such as spot checks or unannounced walk-throughs by supervisors or security personnel, restrictions on items brought into the workplace, confidential complaint channels, or anti-harassment policy, were considered or that such measures would have been ineffective. Nevertheless, even if this second necessity condition were considered satisfied, the Commissioner’s view is that the three-part legitimate interest test would still fail on the third condition, namely the balancing test.

37. The balancing test requires that the controller assesses whether the legitimate interests of the controller and the third parties are overridden by the interests or fundamental rights and freedoms of the complainant. The EDPB has stated the following in Guidelines 3/2019:

“Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party

(e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject.”¹¹.

38. The element of reasonable expectation plays an important role in ensuring the lawfulness of the processing activity. Recital 47 of the Regulation requires that:

*“The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration **the reasonable expectations of data subjects based on their relationship with the controller** ... the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place” [emphasis has been added].*

39. As evidenced by the two photographs submitted by the controller on the 6th January 2026, the controller has affixed CCTV camera signage both outside and inside the canteen. Moreover, the employees were informed of the CCTV system through the controller’s CCTV Policy. The Commissioner notes that this is not sufficient, in itself, to establish that the complainant could reasonably expect to be monitored in the canteen area. The EDPB explains that reasonable expectations do not depend on the information provided to data subjects. Mere compliance with the transparency obligations under the Regulation is not, in itself, sufficient to establish that data subjects can reasonably expect a particular processing activity.¹² In the context of video surveillance, the EDPB has stated that, “[s]igns informing the data subject about the video surveillance have no relevance when determining what a data subject objectively can expect. This means that e.g. a shop owner cannot rely on customers objectively having reasonable expectations to be monitored just because a sign informs the individual at the entrance about the surveillance.”¹³

40. The Commissioner further notes the following extracts from sections 10.1 and 10.4 of the controller’s CCTV Policy: “[t]he **camera/s installed in the Canteen are fixed and their capture zone would be specifically on the machines and equipment and not the area in which**

¹¹ Ibid., paragraph 30.

¹² Guidelines 1/2024 (n 5) paragraph 53.

¹³ Guidelines 3/2019 (n 2) paragraph 40.

employees rest [...] It is the Company's policy not to use video surveillance in areas under "high expectations of privacy" e.g. canteens, toilets and changing rooms, except where the Company feels it is necessary to deter and prevent illicit activities including but not limited to theft, voyeurism or sexual harassment. In any such cases of video surveillance, the Company shall implement security measures to minimise the viewing of spaces/individuals which are not relevant to the legitimate purpose of monitoring, for example, by mounting the cameras in a particular position or using 'privacy masks' i.e. blocking/removing certain areas of a scene from the camera's view" [emphasis has been added]. Accordingly, the controller's own CCTV Policy recognises canteens are areas where there is a high expectation of privacy and states that cameras installed in such areas should be positioned so as to capture company machines and equipment rather than areas in which employees rest. However, from the image grab taken from the footage of the canteen CCTV camera submitted by the controller on the 9th February 2026, it is clear that the camera captures the employees' resting area, as it records the entire room, including the general dining area where employees sit and relax. The actual positioning of the camera therefore appears inconsistent with the controller's stated internal safeguards.

41. Moreover, the Commissioner notes that in his submissions, the complainant argued that his signed acknowledgment of receipt of the CCTV policy predates the installation of the camera in the canteen and that employees were not specifically informed that this rest area would be subject to monitoring. The complainant further submitted that "[e]mployees have a reasonable expectation of a higher level of privacy in such spaces compared to operational or high-risk work areas".
42. According to the former Article 29 Working Party (the predecessor of the EDPB), "[i]n order to rely on [legitimate interest] as the legal ground for processing it is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees. Such measures, depending on the form of monitoring, should include limitations on monitoring so as to guarantee that the employee's privacy is not violated. **Such limitations could be: geographical (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places and for example sanitary zones and break rooms should be prohibited)**..." [emphasis has been added].¹⁴

¹⁴ Article 29 Working Party WP 249 Opinion 2/2017 on data processing at work, adopted on the 8th June 2017, page 7.

43. In another opinion concerning the processing of personal data by means of video surveillance, the former Article 29 Working Party stated, in relation to surveillance in the workplace, that “[t]he implementing experience has shown additionally that **surveillance should not include premises that either are reserved for employees’ private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas...**” [emphasis has been added].¹⁵
44. A similar position has likewise been adopted by the Council of Europe’s advisory body on constitutional matters, the European Commission for Democracy through Law (Venice Commission), as cited by the European Court of Human Rights in the case *López Ribalda and Others v Spain*, concerning workplace surveillance. In particular, the Court quoted the Venice Commission’s statement that “[a]s regards workplaces, the introduction of video monitoring requires respecting the privacy rights of the employees [...] video surveillance would, in general, be allowed to prevent or detect fraud or theft by employees in case of a well-founded suspicion. However, except in very specific circumstances, **videotaping would not be allowed at places such as toilets, showers, restrooms, changing rooms, or smoking areas and employee lounges where a person may trust to have full privacy.**” [emphasis has been added].¹⁶
45. In light of the above, the Commissioner considers that employees reasonably expect a higher degree of privacy in rest areas than in areas dedicated to operational tasks or public access. Continuous recording in such rest areas interferes disproportionately with employees’ rights to privacy and the protection of personal data. Consequently, the use of CCTV in workplace canteens may only be justified under article 6(1)(f) of the Regulation in narrow and exceptional circumstances with strict safeguards and limitations. In the circumstances of the present case, having assessed all submissions, and in the absence of compelling justification, the Commissioner finds that the controller’s interests are overridden by the rights and freedoms of the complainant.

On the basis of the foregoing considerations, the Commissioner hereby decides that the controller could not validly rely on article 6(1)(f) of the Regulation as a legal basis for the processing activity conducted by means of the CCTV camera in the canteen area of its [REDACTED]. The controller further failed to effectively demonstrate that such processing activity is based on one

¹⁵ Article 29 Working Party WP 89 Opinion 4/2004 on the processing of personal data by means of video surveillance, adopted on the 11th February 2004, page 25.

¹⁶ *López Ribalda and Others v Spain* (Apps Nos 1874/13 and 8567/13) (2019) ECtHR (GC) paragraph 61.

of the legal bases set out in article 6(1) of the Regulation. Accordingly, the Commissioner finds an infringement of articles 5(2) and 6(1) of the Regulation.

Pursuant to article 58(2)(f) of the Regulation, the Commissioner is hereby ordering the controller to stop the processing operation and remove the CCTV camera in the canteen area of its [REDACTED] [REDACTED] within twenty (20) days from the date of service of this decision. The controller is hereby ordered to inform the Commissioner of the corrective action taken immediately thereafter, supported by photographic evidence to effectively demonstrate compliance with this order.

In terms of article 83(6) of the Regulation, the controller is hereby informed that non-compliance with this order shall be subject to the appropriate corrective action.

By virtue of article 58(2)(b) of the Regulation, the controller is hereby served with a reprimand.



Ian Deguara
Information and Data Protection Commissioner

Today, the 20th of April, 2026

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 Information and Data Protection Appeals Tribunal shall be addressed to:

The Secretary
Information and Data Protection Appeals Tribunal
158, Merchants Street
Valletta.