Information and Data Protection Commissioner

CDP/COMP/16/2026

[redacted]

vs

[redacted]

COMPLAINT

1. On the 12th of January 2026, Ms [redacted] (the "**complainant**") lodged a data protection complaint with the Information and Data Protection Commissioner (the "**Commissioner**") pursuant to article 77(1) of the General Data Protection Regulation[1] (the "**Regulation**"), alleging that during her stay at the [redacted] (the "**controller**"), an employee misused her personal data. Specifically, the complainant alleged that the mobile number which she provided when booking her accommodation was used by an employee of the controller to send her text messages without her consent, the content of which was unrelated to her booking and stay. The complainant further alleged that this occurred after the controller's employee had already made other attempts to speak to her in person, which she explained "*caused* [her] *significant distress*" and "*made* [her] *feel unsafe*". The complainant alleged that she reported this to the controller, yet no concrete action was taken to address her concerns.

2. For the purpose of supporting her allegations, the complainant submitted **(i)** copies of the text messages which were sent to her by the controller's employee, and **(ii)** a copy of the police report bearing reference number [redacted], which she made on the 5th of January 2026, in which her allegations were recorded.

[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.

[redacted]

[redacted]

INVESTIGATION

Submissions of the controller

3. Pursuant to the internal investigative procedure of this Office, the controller was provided with a copy of the complaint and was given the opportunity to make any submissions it deemed relevant and necessary to defend itself against the allegations made by the complainant.

4. By means of an email sent on the 11th of February 2026, the controller made the following submissions for the Commissioner to consider in the legal analysis of the present case:

    a. that, firstly, the controller sought to premise and underline that the complainant is exaggerating in order to obtain monetary compensation from the controller;

    b. that the complainant's intentions are evidenced from the fact that, in addition to the complaint which she lodged with the Commissioner, she also made other reports or complaints, including with the Malta Police Force, the Malta Tourism Authority, and the Ministry for Foreign Affairs and Tourism;

    c. that the text message which was sent to the complainant by its employee was "*completely innocuous*" and was "*sent purely by mistake*";

    d. that the complainant's mobile number was collected by the controller for "*logistical purposes*", specifically, as it is necessary for the controller to be able to communicate with its guests when they are not present in their rooms, for example, when guests fail to check-out by the pre-established check-out time;

    e. that, hence, no breach was committed by the controller when it requested the complainant to provide her mobile number; and

    f. that, finally, the fact that the complainant was messaged by its employee was unfortunate, however the complainant's reaction to the incident was extreme and was fuelled by her intention to obtain monetary compensation from the controller, which the controller refuses to pay.

Submissions of the complainant

5. The Commissioner then shared the submissions of the controller with the complainant to provide her with the opportunity to respond to and rebut the arguments presented.

6. By means of an email sent on the 11th of March 2026, the complainant made the following submissions which were pertinent to the complaint:

   a. that the complainant considers the submissions put forward by the controller to consist of no more than its own subjective opinion;

   b. that had the controller had more robust policies and procedures in place, the need for the complainant to inform the police and other authorities about the incident would have been reduced;

   g. that when the complainant contacted the Ministry for Foreign Affairs and Tourism about the incident, her allegations were treated with seriousness, and she was instructed to lodge a complaint with the Commissioner;

   h. that while the complainant understands that it is standard practice for hotels to collect certain personal data of their guests, she expected that her personal data would be processed appropriately, particularly in light of there being "*rules as to purpose limitation*";

   i. that the text message she received "*was not a message pertaining to hotel purposes*", and thus, if the controller considers this to have been merely a mistake, then "*evidently, there is some data protection issue that needs reviewing*"; and

   j. that, importantly, although the employee subsequently sent further text messages to the complainant apologising for the initial message, and informing her that it was meant to be sent to another guest in connection with their check-out from the hotel, these were only sent *after* the complainant had reported the incident to another staff member of the controller.

Further clarification sought by the Commissioner

7. After reviewing the submissions provided by both the controller and the complainant, the Commissioner determined that further clarification was needed from the controller regarding its established practices for communicating with its guests. To this end, the Commissioner posed a series of questions to the controller, namely:

QUOTE

i. *Whether the controller (i.e., the hotel) has in place a formal policy and/or procedure regarding how to communicate with guests, and if so, whether the policy specifies any approved channels of communication;*

ii. *Whether employees are permitted to use their mobile devices when communicating with guests, and if so, under what conditions is this permission granted;*

iii. *Whether the employee had access to the guest's mobile number by reason of his role, and the details of the employee's role;*

iv. *Whether the text messages which were sent by the employee regarding the guest's late checkout were sent on the instructions of the controller; and*

v. *Whether there are any safeguards in place to protect the personal data of guests, including the provision of training to employees on how to handle personal data in the course of performing their role.*

END QUOTE

8. In response, on the 6th of April 2026, the controller submitted the following replies:

   a. As to whether the controller has in place a formal policy and/or procedure regarding how to communicate with guests, and if so, whether it specifies any approved channels of communication – the controller replied that the hotel in question is only a small boutique hotel employing seven (7) people, and that the hotel's policy is that communications with guests are "*ideally made by the manager of the hotel*";

   b. As to whether employees are permitted to use their mobile devices when communicating with guests, and if so, under what conditions – the controller replied that the manager of the hotel is permitted to use his personal mobile device to communicate with guests "*on a strictly as-necessary basis*";

c. As to whether the employee had access to the mobile number by reason of his role, and the details of the employee's role – the controller replied that, indeed, the employee had access to the mobile number as he is the manager of the hotel;

d. As to whether the text messages which were sent by the employee regarding the guest's late checkout were sent on the instructions of the controller – the controller replied that since the employee is the manager of the hotel and his role consists of managing the day-to-day operations of the hotel, he does not receive instructions on day-to-day matters from anyone; and

e. As to whether there are any safeguards in place to protect the personal data of guests, including the provision of training to employees on how to handle personal data in the course of performing their roles – the controller replied that its employees are instructed not to use guests' personal data for any reason other than in connection with their stay at the hotel.

Finally, the controller reiterated its belief that the complainant's actions are motivated by a desire to obtain monetary compensation from the controller, and maintained that the message was sent by mistake and that the manager has since apologised to the complainant.

LEGAL ANALYSIS AND DECISION

The alleged misuse of the complainant's personal data

9. In her complaint, the complainant alleged that the mobile number which she provided when booking her accommodation with the controller was subsequently used for a purpose entirely unrelated to the one for which it had originally been processed. The complainant specified that the misuse of her personal data occurred when an employee of the controller, namely, the hotel manager, used the mobile number collected by the controller to send her text messages from his personal mobile number, without her consent, the content of which was unrelated to her booking or stay. Accordingly, the Commissioner began by assessing the copies of the text messages which the complainant had submitted in support of her complaint, which demonstrated that:

a. on the 4th of January 2026, at 17:13, the complainant received a text message from a mobile number she was not familiar with, containing solely a smile emoji. The complainant did not respond to the text message;

b. at 19:55, nearly three (3) hours later, the complainant received another text message from the same mobile number, stating that the initial text message was sent by mistake, and was meant to be sent to another guest in connection with their check-out from the hotel. The complainant identified the sender as an employee of the controller, namely, the manager;

c. at 20:12, the complainant responded, informing him that his text message had made her feel unsafe and that he did not have permission to contact her; and

d. at 20:15pm, the employee responded by further apologising to the complainant, and reiterated that he sent the earlier text message by mistake.

10. Upon reviewing the content of the text messages, the Commissioner made a number of key observations. Notably, the messages originated from the manager's personal mobile number, and not from an official business number of the controller. Additionally, although the manager maintained that the first text message was intended to be sent to another guest in connection with their check-out from the hotel, the message contained no information whatsoever pertaining to the other guest or their check-out. Furthermore, the Commissioner also considered that in her submissions, the complainant submitted that the further text messages which were sent hours later – namely, in which the manager stated that the initial message was sent by mistake – were only sent *after* the complainant had formally reported the incident to another staff member of the controller.

11. Pertinently, the Commissioner noted that when requested to put forward its submissions on the complaint, the controller failed to present any concrete evidence or persuasive line of argumentation to rebut the complainant's allegation regarding the misuse of her personal data. Rather, the controller simply submitted that the text messages received by the complainant were "*completely innocuous*" and "*sent purely by mistake*". In this regard, the Commissioner referred to article 5(1)(b) of the Regulation, which places a clear obligation on the controller to ensure that the personal data is not processed for a purpose that is incompatible with the purpose for which it was initially collected, in line with the principle of purpose limitation. Accordingly, the processing of personal data for an objective which is distinct from that for

which it was collected, and which is incompatible with that objective, would constitute a misuse of that personal data. In its submissions, the controller further explained that the complainant's mobile number was collected for "*logistical purposes*", as it is necessary for the hotel to be able to communicate with its guests when they are not present in their rooms, for example, where guests fail to check-out by the pre-established check-out time. In this regard, the Commissioner considered that the collection of guests' mobile numbers could indeed be regarded as being necessary in relation to the purpose identified by the controller, particularly to cater for situations where a guest cannot be reached via the telephone located in their hotel room, and having the guest's contact details on file is necessary to be able to contact that guest directly. Accordingly, the Commissioner considered that, in principle, the complainant's personal data was collected by the controller in pursuit of a legitimate purpose. However, the personal data was ultimately used for a different purpose, as the message received by the complainant, and the context in which it was sent, was not related to her booking nor in any manner to her stay at the hotel.

12. Finally, the Commissioner considered that during the course of the investigation, the controller failed to present any documented evidence to substantiate its position that it acted in compliance with the Regulation and to rebut the complainant's allegation regarding the misuse of her personal data. In this regard, the Commissioner considered it pertinent to draw the controller's attention to the overarching principle of accountability under article 5(2) of the Regulation, which explicitly states that the controller is responsible not only for complying with the Regulation, but also for being able to demonstrate its compliance in practice. Accordingly, in the event that a data protection issue arises, the controller must be in a position to actively demonstrate, including by providing documented evidence and records, that it has acted in accordance with the Regulation, and that it has in place effective measures and safeguards to mitigate the likelihood of infringements of the Regulation.

The practices of the controller

13. As the second part of the legal analysis of the present case, the Commissioner had to assess whether the practice maintained by the controller for communicating with its guests complied with the Regulation. During the course of the investigation, when the Commissioner requested further clarification from the controller in this regard, the controller confirmed that where it is necessary to contact a guest in connection with their stay at the hotel, the guest may be contacted by an employee of the controller – ideally being the hotel manager – using his or

her own mobile device. Although the Commissioner explicitly requested the controller to confirm whether it has a formal policy in place that regulates how guests are to be contacted and what the approved channels of communication are, the controller failed to share any such policy with the Commissioner. Accordingly, the Commissioner considered that the practice adopted by the controller was not documented in any formal policy regulating the manner for communicating with guests, but was merely adopted informally, without there being any real justification for doing so under the Regulation.

14. Pertinently, in making his assessment, the Commissioner referred to the EDPB (the "**European Data Protection Board**") Guidelines 4/2019 on Article 25 – Data Protection by Design and Default[3], which explain *inter alia* that processing operations must be considered as 'necessary' in order to be lawful under the Regulation. In particular, the Guidelines emphasise that in making an assessment as to whether an envisaged processing operation is necessary, the controller must carefully consider whether it would be "*within the reasonable expectations of data subjects*".[4] If the particular processing operation does not fall within the data subjects' reasonable expectations, the controller would have to consider whether there may be other suitable processing operations that could effectively achieve its intended objective. In this regard, the Guidelines further explain that merely because it may be necessary for the controller to collect certain personal data to achieve an identified purpose, this does not imply that all types of processing operations may subsequently be carried out on that personal data.[5]

15. In the present case, the controller submitted that "*there was no breach* [...] *by the fact that* [the complainant's] *mobile number was requested*" by the controller. Taking into account the guidance provided by the EDPB, the Commissioner reiterated that the *initial collection* of guests' mobile numbers could indeed be regarded as necessary in relation to the purpose identified by the controller, particularly to cater for situations where a guest cannot be reached via the telephone located in their hotel room, and having the guest's contact details on file is necessary to be able to contact that guest directly. However, the controller failed to demonstrate how the *subsequent use* of the personal data in the manner described, namely, by allowing the manager to contact guests using his own personal mobile device, could be considered as being a necessary course of action that is within the reasonable expectations of the data subjects. The Commissioner stressed that the controller has official and appropriate communication channels

[3] EDPB Guidelines 4/2019 on Article 25 – Data Protection by Design and Default, adopted on the 20th of October 2020.
[4] Ibid, paragraph 51.
[5] Ibid, paragraphs 48 and 51.

at its disposal through which its intended objective could have been achieved, including, for example, by sending an email to the guest from the controller's official email address, or calling the guest from the hotel's reception desk or other official business phone number. The Commissioner considered that while the complainant could reasonably expect to be contacted through these official channels, it would not be reasonable for her to expect to receive communications originating from the personal phone number of an employee, nor for her mobile number to be stored on an employee's personal mobile device, even if that employee were to be a senior staff member, such as a manager. Accordingly, the Commissioner determined that the controller's current practice for communicating with its guests via the personal mobile number of the employee, did not fall within the data subjects' reasonable expectations, was not necessary, and consequently, was unlawful under the Regulation.

16. The Commissioner also referred to a recent judgement of the Court of Justice of the European Union (the "**CJEU**"), namely, *GP vs. Juris GmbH*, in which the CJEU clarified the extent of controllers' responsibility for infringements caused by the wrongful conduct of employees, and highlighted the importance for controllers to ensure compliance with their data protection obligations, in particular those set out under articles 24, 25, and 32 of the Regulation, in order to prevent the occurrence of such breaches.[6] This includes the controller's obligations to implement appropriate technical and organisational measures to ensure processing is carried out in accordance with the Regulation – including by implementing data protection policies to this end[7], and giving training to its employees, as well as the controller's obligations to ensure that the extent of its processing activities are limited to what is necessary for the purpose of processing, by default,[8] and to ensure the security of the personal data undergoing processing.[9] The CJEU held that unless the controller can demonstrate that it has fully complied with its data protection obligations, the controller is deemed to have participated in and is responsible for the processing causing the breach. Thus, the Commissioner concluded that by maintaining such a practice, and failing to have in place any formal policy regulating how communications with guests are to be made, the controller failed to comply with its data protection obligations, and effectively created a situation where guests' personal data could easily be misused by employees.

[6] Case C-741/21, GP vs. Juris GmbH, judgement of the Court of Justice of the European Union (Third Chamber) of the 11th of April 2024, paragraph 50.
[7] Article 24(1) and (2) of the Regulation.
[8] Article 25(2) of the Regulation.
[9] Article 32 of the Regulation.

On the basis of the foregoing considerations, the Commissioner is deciding, firstly, that the complainant's personal data was processed for a different purpose than that for which it was collected, as the message received by the complainant, and the context in which it was sent, was not related to her booking nor in any manner to her stay at the hotel, and secondly, that the practice maintained by the controller for the purpose of communicating with its guests does not comply with the requirements of the Regulation, and facilitated abuse of the guests' personal data by employees.

For this reason, the Commissioner is ordering the controller to immediately cease its current practice, and to establish a new procedure for communicating with its guests which complies with the Regulation, and which utilises exclusively official communication channels of the controller to do so.

The Commissioner is also ordering the controller to document this procedure through a formal internal policy, and to give proper training to its employees who have access to personal data by reason of their role, so as to ensure that they are processing personal data in a manner that complies with the Regulation.

Information and Data Protection Commissioner

Decided today, the 20th of April 2026.

Right of Appeal

You are hereby being informed that in terms of article 26(1) of the Data Protection Act (Chapter 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.[10]

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*".

[10] Further information is available on the IDPC's portal at the following hyperlink: https://idpc.org.mt/appeals-tribunal/