Information and Data Protection Commissioner

CDP/COMP/960/2023

[redacted]

vs

[redacted]

COMPLAINT

1. On the 23rd of November 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**" or the "**GDPR**"). alleging that [redacted] (the **"controller"** or the "**hotel"**) "*asked for my identification document. I presented my passport, after which that employee handed the passport to another staff member, who made a photocopy of it*". Moreover, the complainant contends that the "*hotel's staff did not inform me about their intention to make a copy of my passport or about personal data collection this way. They did not ask my permission to do that, nor did they have my consent to perform that action*". The complainant claimed that after accessing the privacy policy available on the website of the controller, he "*could not find anything regarding data collection by copying guests' passports*".

INVESTIGATION

Request for submissions

2. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with the opportunity to provide any information which it deemed relevant and necessary to defend itself against the allegation raised by the complainant. By means of an email dated the 19th of February 2024, the controller submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:

[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).

a. that the controller does not scan and upload the passport onto its system, and instead, the copy remains as a physical document along with the registration card for the duration of the retention period, and following this period, both documents are properly shredded; and

b. that the controller does not possess or utilise any facial recognition devices to identify individuals solely from their images, and consequently, the controller asserts that an image alone does not constitute a special category of personal data.

3. Moreover, the controller submitted its Privacy Impact Assessment (the "**PIA**") outlining a more detailed assessment of the processing activity. The PIA evaluates the privacy risks associated with the collection, storage, and handling of the guests' personal data, particularly, the identity documents. The assessment found that collecting personal data, including copies of identity documents, is essential for the safety of the guests and the security of the hotel.

4. The PIA explains that personal data, such as passport details and scanned identity documents, are collected upon check-in for the purpose of verifying the identity of guests, ensuring the security of guests and hotel premises, and safeguarding the financial interests of the hotel. The processing of these data is justified in terms of the legal obligations which the controller is subject to, in terms of article 6(1)(c) of the Regulation. This is namely by virtue of article 24 of the Malta Travel and Tourism Services Act (Cap. 409 of the Laws of Malta) and article 31 of the Immigration Act (Cap. 217 of the Laws of Malta). The PIA further explains that such processing is necessary for the purpose of pursuing the legitimate interest of the controller under article 6(1)(f) of the Regulation, that is, verifying personal details, ensuring efficient check-in, preventing fraud, and defending legal claims. Despite potential risks, such as data breaches and misuse of passport data for identity fraud, mitigation measures are in place, including staff training, access controls, secure data retention, and clear provision of information to guests. The PIA concludes that the collection and processing of personal data by the controller are conducted in compliance with the regulations and with due consideration for privacy protection, ensuring safety and security with appropriate safeguards to mitigate any privacy risks.

5. The Commissioner provided the complainant with the opportunity to rebut the submissions of the controller. By means of an email dated the 11th of March 2024, the complainant submitted the following salient arguments for the Commissioner to consider during the legal analysis of the present case:

a. that the PIA does not provide any legal basis for the extensive collection and processing of personal data by photocopying two pages of the passport without his consent;

b. that article 24 of the Malta Travel and Tourism Services Act and article 31 of the Immigration Act do not authorise the controller to collect a copy of the guests' identity documents or passports; and

c. that the data collection and processing occurred without his consent, as he objected to the hotel's staff actions immediately upon observing them, and consequently, the controller has not sufficiently demonstrated a lawful basis for obtaining and processing his personal data in the manner complained of.

6. On the 27th of March 2024, the controller submitted a copy of its Legitimate Interest Assessment (the "**LIA**") for such processing and provided that the LIA together with the previously provided PIA, amply supports the position of the controller to pursue its legitimate interests in processing the underlying personal data during the registration process.

7. The controller asserted that the processing of personal data under article 6(1)(f) of the Regulation does not require the data subject's consent, which is instead addressed under article 6(1)(a) thereof. Furthermore, section 10.2 of the Privacy Notice of the controller[2] clearly and transparently informs the data subjects of their rights. These rights include the ability to object, which is limited to the withdrawal of consent for the use of personal information for marketing purposes, as well as for profiling and automated decision-making, where applicable.

LEGAL ANALYSIS AND DECISION

8. For the purpose of this complaint, the Commissioner examined the contents of the complaint and proceeded to determine: (a) whether the controller had a legal basis in terms of article 6(1) of the Regulation to collect a copy of the passport document of the complainant during its guest registration process and to subsequently store such copy; and (b) whether the controller had provided information to the complainant about the collection and storage of the copy of the passport document.

[2] Accessible at: https://www[redacted]ivacy-policy/

The lawfulness of the processing

9. The Commissioner highlights that every processing operation which falls within the meaning of article 4(2) of the Regulation should invariably be legitimised on the basis of a legal ground in terms of article 6(1) of the Regulation. Pursuant to the principle of accountability as set forth in article 5(2) of the Regulation, the onus rests upon the controller to effectively demonstrate that the processing fully complies with the provisions of the Regulation.

10. The Court of Justice of the European Union (the "**CJEU**") held that "*Article 7 of Directive 95/46* ***sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful*** *and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article*"[3]. In a recent judgment, the CJEU reaffirmed that "*it must be pointed out that any processing of personal data … must satisfy* ***the conditions of lawfulness set by Article 6 of the GDPR***"[4] [emphasis has been added].

11. It therefore follows that the processing of personal data is deemed to be lawful if it comes within at least one of the six grounds as mentioned in article 6(1) of the Regulation, which are as follows: (a) consent; (b) contract; (c) compliance with a legal obligation; (d) vital interest; (e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (f) legitimate interest. In the present case, the controller had to concretely demonstrate that the processing of the personal data pertaining to the complainant was based on at least one of these legal grounds set forth in article 6(1) of the Regulation. During the course of the investigation, the controller argued that the processing, which includes the collection and storage of the passport document of the complainant, is based on article 6(1)(c) and article 6(1)(f) of the Regulation.

Article 6(1)(c) of the Regulation

12. Article 6(1)(c) of the Regulation is one of the legal grounds that enables the controller to process personal data if it "*is necessary for compliance with a legal obligation to which the controller is subject*". The legal obligation must originate directly from national or Union law. The provision which defines the legal obligation does not need to be specific to each individual

[3] Case C-582/14, Patrick Breyer vs Bundesrepublik Deutschland, decided on the 19th October 2016, para. 57.
[4] Case C-268/21, Norra Stockholm Bygg AV v Per Nycander AB, decided on the 2nd March 2023, para. 29.

processing, however, it must be sufficiently clear, precise, and foreseeable and, in particular, it should define the purposes of the processing[5].

13. In this case, the controller submitted that the processing is justified under article 6(1)(c) of the Regulation in view of legal obligations to which it is subject, deriving from article 24 of the Malta Travel and Tourism Services Act (Cap. 409 of the Laws of Malta) and article 31 of the Immigration Act (Cap. 217 of the Laws of Malta).

14. The Commissioner proceeded to examine article 24 of the Malta Travel and Tourism Services Act (Cap. 409 of the Laws of Malta), which provides that:

> "[e]*very hotel keeper, guest house keeper, hostel keeper, and keeper of holiday premises shall keep a register in the prescribed form wherein he shall cause every guest to write his name together with such other particulars as may be prescribed*".

15. In addition to the foregoing, the Commissioner assessed article 31 of the Immigration Act (Cap. 217 of the Laws of Malta), which provides that:

> "*(1) It shall be the duty of the keeper of any premises to which this article applies to keep a register of all persons staying at the premises who are not exempt persons.*
>
> *(2) The keeper of any premises to which this article applies shall, on the arrival of any person who is not an exempt person, ascertain and enter or cause to be entered in the register kept for the purpose the name and nationality of such person, together with the date of his arrival and the address from which he last came; and on departure of any such person the keeper of the premises shall enter or cause to be entered in the register the date of departure and the destination on departure of that person.*"

16. These provisions impose an obligation on the controller to maintain a register of guests and authorise the controller to request the guests to provide their name, and any other particulars, which include, the nationality, together with the arrival and departure date, and the address from which the guests last came and the destination on their departure. The law is clearly specifying

[5] *Heberlein*, in Ehmann, Selmayr, Datenschutz-Grundverordnung, Article 6 GDPR, margin number 15 (C.H. Beck 2018, 2nd Edition).

which information must be collected by the controller from the guest, and such provision does not oblige the controller to collect and store copies of the passport document . Given the very prescriptive nature of these provisions, particularly article 31(2) of Cap. 217, the Commissioner could not accept the argument of the controller that the law could serve as a legal basis to collect and store copies of the passport document.

Article 6(1)(f) of the Regulation

17. Article 6(1)(f) of the Regulation provides that the processing is lawful 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*".

18. The case-law of the CJEU reiterated on a number of occasions that a controller may rely on article 6(1)(f) of the Regulation if it satisfies the three-part test[6]. In particular, the CJEU in the landmark ruling of Rigas stated that:

> "*In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.*"[7]

19. In this respect, the Commissioner assessed the present case in the light of the three (3) cumulative conditions as laid down by the CJEU. All the three (3) conditions identified by the CJEU need to be present: (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.

20. First, the processing is conditional upon the existence of a legitimate interest of the controller or of a third party. The Regulation does not define legitimate interest, and thus, it is for the

[6] C-13/16, Rigas satiksme, paragraph 28 and C-708/18 TK v Asociația de Proprietari bloc M5A-ScaraA, paragraph 40.
[7] C-13/16, paragraph 28.

controller to determine whether there is a legitimate aim that could justify an interference with the right to the protection of personal data.

21. 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 and this could be, 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, for the purpose of preventing fraud, the transmission of certain data within groups of companies and processing for the purpose of ensuring network and information security.

22. In the present case, the condition relating to the existence of a present and effective interest seems to be fulfilled, since the controller submitted documentary evidence, specifically the LIA and the PIA, which demonstrates that the controller has legitimate interests to process such personal data for security reasons and to defend itself against any legal claim. The controller explained that verifying the identity of guests helps maintain a secure environment within the hotel and prevents fraudulent activities. Several times, the Malta Police Force has requested identification documents from the controller to assist in investigations related to fraud or other security incidents within the hotel premises. Moreover, the controller held that there have been instances in the past where guests have tried to leave the hotel without settling all outstanding fees and expenses, caused damages that were not immediately noticeable during check-out, or made claims of wrongful payment via the credit card charge-back mechanism, which allows clients up to 90 days to contest a transaction. Therefore, a copy of the passport, along with the registration card, would support the hotel's defence by proving that the individual was indeed a guest during a specific period.

23. Within this context, the Commissioner carefully assessed the wording of recital 47 of the Regulation, which provides that "*[t]he processing of personal data strictly necessary for the purposes of* ***preventing fraud*** *also* ***constitutes a legitimate interest of the data controller concerned***" [emphasis has been added].

24. The Commissioner is of the view that the collection and storage of the copies of passports of guests assist the controller in preventing fraudulent activities, such as identity theft or misuse of hotel services by individuals using false identities. This is especially important in the hospitality industry where services are often provided upfront before payment, making fraud

prevention a legitimate and reasonable concern for hotels. Consequently, the Commissioner is of the view that the processing of personal data for the purpose of fraud prevention could serve as a legitimate interest of the controller.

25. In relation to the second condition of the legitimate interest test, the Commissioner proceeded to determine whether the processing of personal data pertaining to the complainant was indeed necessary for the purpose of the attainment of the legitimate interest at issue. In this regard, the Commissioner noted that the principle of data minimisation as laid down in article 5(1)(c) of the Regulation requires that the processing shall 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 should be limited to what is plausibly necessary to pursue the legitimate interest, and, therefore, there should be a connection between the processing and the interest pursued.

26. The CJEU in the 'TK vs Asociaţia de Proprietari bloc M5A-ScaraA' held that the necessity test must consist, in essence, in ensuring that the legitimate interest "*cannot reasonably be as effectively achieved* ***by other means less restrictive*** *of the fundamental rights and freedoms of the data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Article 7 and 8 of the Charter*"[8] [emphasis has been added].

27. The Commissioner emphasises that the onus rests upon the controller to concretely demonstrate how it conducted the legitimate interest test in terms of the principle of accountability as set forth in article 5(2) of the Regulation. In this case, the controller provided the Commissioner with an explanation that its intended objective could not reasonably be achieved by other means less restrictive of the fundamental rights and freedoms of the complainant. In this regard, the Commissioner deems the processing activity conducted by the controller to be necessary and proportionate in relation to the interest pursued.

28. Lastly, as regards the third condition laid down in article 6(1)(f) of the Regulation, relating to the existence of fundamental rights and freedoms of the data subject whose data require protection, which might override the legitimate interests pursued by the controller, it is relevant to emphasise that the assessment of that condition necessitates a balancing of the opposing rights and interests concerned. The controller must conduct a balancing test to ensure that its legitimate interests in processing the copies of passport documents do not override the interests or fundamental rights and freedoms of the guests. This includes considering the potential impact

[8] C-708/18, paragraph 47.

on guests' privacy and ensuring that the data processing is proportionate to the intended purposes.

29. The Commissioner proceeded to further evaluate the LIA and the PIA submitted by the controller, whereby according to the controller, the outcome of the balancing test indicated that legitimate interests justify this processing activity.

30. After assessing the nature of the data processed, the context of the processing and the impact of the processing on the data subjects, the Commissioner concludes that the processing activity conducted by the controller fulfills all the conditions set forth in article 6(1)(f) of the Regulation as the purposes are aligned with the legitimate interests of security, fraud prevention, and enhancing guest services.

Transparency

31. After the Commissioner determined that the controller had a lawful basis in terms of article 6(1)(f) of the Regulation to collect and store the copy of the passport of the complainant, the Commissioner proceeded to examine the allegation raised by the complainant, namely, that the controller failed to provide appropriate information in relation to the processing activity at the time of collection of his personal data.

32. Article 13(1) of the Regulation obliges the controller that where personal data are collected from the data subject, the controller shall provide the individual with all the information prescribed in article 13(1) and article 13(2) of the Regulation. The Regulation clearly stipulates that the information shall be provided "*at the time when personal data are obtained*" from the data subject. In the present case, the Commissioner noted that the copy of the passport document was requested at the time of the complainant's check-in at the hotel, and therefore, the relevant information regarding the processing should have been provided to the complainant at the time when his copy of the passport was collected.

33. The Commissioner has considered the 'Guidelines on Transparency under Regulation 2016/679' (the "**Guidelines**") issued by the Article 29 Working Party, which have been endorsed by the EDPB. These Guidelines underscore the importance of the controller providing information about the processing in a timely manner, which is necessary to enable the controller to comply with the principles of transparency and fairness. The Guidelines outline these scenarios as examples of when the information in relation to the processing should be provided to the data subject at the time of collection of the personal data:

> "*By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained*".

34. The Guidelines provide further examples as to the methods that the controller may use to provide the information to the data subject in a non-digital setting, such as in the present case where the interaction took place in person:

> "*A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject.* ***For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.***" [emphasis has been added].

35. The Regulation does not specify the modality or format by which the information prescribed in article 13 must be provided to the data subject, however, it does clearly assign the responsibility to the controller to implement the appropriate measures to ensure that the data subjects receive the information in a timely manner. The Guidelines recommend that in case of person-to-person interaction, the controller may provide the most important information verbally during the interaction, followed by a complete data protection notice that contains all the requirements set forth in article 13 of the Regulation. This may include sending the notice via email, providing a QR code that links directly to the notice or by providing a physical copy of the notice.

On the basis of the foregoing considerations, the Commissioner is hereby deciding that:

i. **the controller lawfully processed the copy of the passport document pertaining to the complainant pursuant to article 6(1)(f) of the Regulation; and**

ii. **the controller failed to take appropriate measures to provide the complainant with all the information referred to in article 13 of the Regulation at the time when the personal data were obtained from the complainant.**

In accordance with article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to develop an internal procedure or policy that outlines an appropriate measure to ensure that the controller provides the data subjects with all the information set forth in article 13 of the Regulation at the time of collection of their personal data. The controller shall comply with this order within one (1) month from the date of the service of the decision and information on the action taken to comply with this order shall be provided immediately thereafter.

Failure to comply shall lead to the appropriate corrective action pursuant to article 83(6) of the Regulation.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2025.01.20 14:13:55 +01'00'

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

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 in writing to the Tribunal within twenty days from the service of the said decision as provided in article 23"*.

An appeal to the Information and Data Protection Appeals Tribunal shall be made in writing and addressed to "*The Secretary, Information and Data Protection Appeal Tribunal, 158, Merchants Street, Valletta*[9].

[9] More information is available on our portal and accessible at this link: https://idpc.org.mt/appeals-tribunal