INFORMATION AND DATA PROTECTION COMMISSIONER

Information and Data Protection Commissioner

CDP/COMP/561/2024

[redacted]

vs

[redacted]

COMPLAINT

1. On the 2nd September 2024, [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 the [redacted] (the "**controller**") processed her personal data in a manner that infringes the provisions of the Regulation.

2. The complainant submitted the following information in connection with the complaint:

   a. that, on the 2nd July 2024, the complainant visited the office of an insurance company to perform the transfer of a vehicle, however, after having finalised the insurance paperwork, the insurance company could not proceed with the transfer using its account in the system of the controller because the ID card number of the complainant was found to be assigned to a different person; and

   b. that, subsequently, the complainant visited the offices of the controller, and the controller proceeded to correct the personal data of the complainant and completed the transfer of the vehicle.

[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.

INVESTIGATION

3. Pursuant to the internal investigative procedure, the Commissioner provided the controller with a copy of the complaint and enabled the controller to provide its submissions that are deemed to be necessary and relevant for the purpose of enabling the controller to defend itself against the allegation raised by the complainant. Following several reminders and follow-ups by this office, the controller delivered by hand a letter dated the 7th May 2025, which was received by this Office on the 13th May 2025. The controller submitted the following arguments for the Commissioner to consider during the legal analysis of this case:

    a. that an internal investigation was conducted by the controller, which confirmed that the error occurred due to a manual data entry mistake, and that as a result of this error, the identity card number of the complainant was erroneously recorded in the vehicle registration database of the controller instead of the correct identity card number;

    b. that the incorrect number of the complainant was erroneously linked to a third party, which previously owned a vehicle from the 28th August 2019 to the 27th August 2021;

    c. that the controller established that the incorrect ID entry was manually inputted into the system, and was later amended on the 2nd July 2024, however, due to database limitations, it was not possible to determine the identity of the user who originally created the incorrect record;

    d. that upon verification of the transfer of ownership documents relating to the vehicle associated with the third party, it was confirmed that all details, including signatures, ID card numbers, and the local insurance policy, were correct, and the controller confirmed that no fraudulent activity or data misuse was detected;

    e. that once the discrepancy was identified by the controller, all incorrect data were rectified, and the system now accurately reflects the correct details;

    f. that the controller acknowledges the importance of ensuring data accuracy in compliance with article 5(1)(d) of the Regulation, which mandates that personal data shall be kept accurate and, where necessary, up to date;

g. that whilst the incident was caused by a human error, the controller has taken corrective actions to mitigate the risk of recurrence, and these include the implementation of additional verification steps before new entries are recorded and a review of internal data input procedures to reinforce compliance with the principles of the Regulation;

h. that, furthermore, the controller is currently evaluating the feasibility of enhancing the database structure to enable traceability of manual data entries by logging user activity at the data creation stage and this will allow for greater accountability in the event of any future discrepancies;

i. that, in addition, the controller is assessing the implementation of automated validation mechanism to cross-reference ID numbers against a centralised identity database before they are stored in the system; and

j. that, finally, the controller submits that this incident resulted from an isolated administrative error, which was promptly rectified, and that no evidence suggests intentional misuse of personal data, however, the controller remains committed to improve its data handling procedures and ensure full compliance with the Regulation.

Further clarifications sought from the controller

4. By means of an email dated the 15th May 2025, pursuant to article 58(1)(e) of the Regulation, the Commissioner ordered the controller to provide information regarding the "*implementation of additional verification steps before new entries are recorded and a review of internal data procedures to reinforce compliance with GDPR principles*". To this end, the Commissioner requested the controller to clearly indicate which additional verification steps were introduced and how the internal data procedures were amended to prevent any incidents of a similar nature.

5. Following several reminders, the controller provided the following reply on the 19th June 2025:

a. that "*new audit checks were included in the tender document for the new* [redacted] *software because the current version lacks any auditing mechanism for the creation of IDs*";

b. that "[t]*his particular case was highly unusual. After a transfer or registration, insurance companies typically verify and update the registration number on their end and promptly notify us of any discrepancies. Moreover, such incidents are extremely rare – we cannot recall any similar cases apart from this one*"; and

c. that "[h]*owever, given the residential permits for non-EU residents have been more prone to errors, we have started requesting a copy of the passport to cross-check and confirm the provided details*".

Consultation with [redacted]

6. Pursuant to article 15(3) of the Data Protection Act (Cap. 586 of the Laws of Malta), the Commissioner consulted [redacted] in the exercise of his functions under the Regulation and requested [redacted] to check to whom the identity card number of the complainant is linked to within its systems. After conducting the necessary checks, [redacted] informed the Commissioner that "[a]*ccording to our records,* [redacted] *is a Maltese National and the holder of ID Card No.* [redacted] *She is registered to be residing at this postal address* [redacted]. Therefore, the Commissioner confirmed that [redacted] was processing accurate personal data in relation to the complainant.

LEGAL ANALYSIS AND DECISION

7. Before proceeding to assess the merits of the case, the Commissioner wishes to highlight the significant lack of cooperation exhibited by the controller during the course of the investigation, particularly evidence in the excessively delayed response of the controller. Article 31 of the Regulation imposes an obligation on the controller to cooperate with the Commissioner whilst performing his investigative tasks as set out in article 57(1)(f) of the Regulation. For this reason, it is imperative that the controller provides timely and comprehensive responses to facilitate an effective investigation. This lack of cooperation is particularly concerning given that the controller is a public authority responsible for the processing of large volumes of personal data. In such circumstances, it is reasonable to expect the controller to respond promptly to requests for information from the Commissioner. Its failure to do so not only cause unnecessary delays to the investigation but also raises serious doubts about the controller's commitment to fulfilling its obligations under the Regulation.

8. The Commissioner proceeded to examine the subject-matter of the complaint, which relates to the allegation that the identity card number of the complainant, contained within the controller's information system, was linked to a third party. Throughout the investigation of the Commissioner, the controller submitted that the error resulted from a manual data entry error, which led to the complainant's identity card document to be erroneously linked to a third party. The Commissioner considered the similarity between the two numbers and accepted that this was indeed a genuine error made by the employee of the controller. In fact, the controller proceeded to amend such incorrect data entry on the 2nd July 2024, after such error was flagged by the complainant. While human errors are bound to happen and may result from inattentiveness or negligence on the part of the employees, or any other factors, the Commissioner expresses significant concern over the statement of the controller that, due to database limitations within its system, it was not possible to identify the user who originally created the incorrect record.

9. The Commissioner is of the view that the inability to trace user activity suggests a failure on the part of the controller to implement the appropriate security measures as required by the Regulation. In fact, the European Data Protection Board (the "**EDPB**") in its Guidelines 4/2019[2] emphasises that data protection by design requires mechanisms, such as logging to be embedded into the processing to ensure compliance with the principle of integrity and confidentiality and to be able to demonstrate compliance with the Regulation. The EDPB considers that one of the key aspects of the principle of integrity and confidentiality includes the keeping of the "*logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control*". Furthermore, the EDPB in its Guidelines 1/2021[3] notes that inadequate logging and user access records can seriously impair a controller's ability to respond to security incidents in the most effective manner.

10. During the investigation, the controller informed the Commissioner that it addressed this shortcoming by incorporating updated specifications into the tender document, ensuring that the new software includes appropriate auditing mechanism. Such a mechanism is essential to substantiate user activity within the system, enabling traceability, demonstrating accountability, and compliance with the requirements of the Regulation.

11. As an additional step to prevent the processing of inaccurate personal data, the controller submitted that "*given the residential permits for non-EU residents have been more prone to*

[2] Guidelines 4/2019 on Article 25 Data Protection by Design and Default, Version 2.0, adopted on the 20th October 2020.
[3] Guidelines 01/2021 on Example regarding Personal Data Breach Notification, Version 2.0, adopted on the 14th December 2021.

errors, we have started requesting a copy of the passport to cross-check and confirm the provided details". The Commissioner emphasises that verification checks form an integral part of ensuring the accuracy of the processing of personal data, however, the controller must ensure that copies of passports are not retained for the sole purpose of verifying personal data. For this purpose, it is sufficient to visually inspect the document and record its relevant details which are strictly necessary for the purpose of the processing conducted by the controller.

On the basis of the foregoing considerations, the Commissioner is hereby deciding that the incident which led to the personal data of the complainant being linked to a third party was the result of a human error, specifically due to an employee incorrectly inputting the personal data of a third party.

Pursuant to article 58(2)(b) of the Regulation, the Commissioner is hereby serving the controller with a reprimand for its failure to cooperate with the Commissioner in a timely manner, and therefore, infringing article 31 of the Regulation. The controller is further warned that a recurrence of such conduct will result in the imposition of an effective, proportionate and dissuasive administrative fine.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2025.06.23 16:34:19 +02'00'

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

The parties are hereby being informed that in terms of article 26(l) 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.[4]

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"*.

[4] Further information is available on https://idpc.org.mt/appeals-tribunal/.