Information and Data Protection Commissioner

CDP/COMP/427/2025

[redacted]

vs

[redacted] **Local Council**

COMPLAINT

1. On the 6th August 2025, [redacted] (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 Regulation[1] (the "**Regulation**"), alleging that the [redacted] Local Council (the "**controller**") infringed her right to the protection of personal data when it unlawfully disclosed her personal data to a third-party company.

2. The complainant submitted that "*I called the local council, about a problem regarding a construction company, which was closing our garages without any notice (happened more than once). The local council contacted the mentioned construction company and advised them that I reported them, and gave them my Name and Surname, my email, my mobile number, and my address. Without asking for my permission. Obviously this can lead to negative things being done to me.*". As supporting documentation, the complainant submitted a screenshot of the email correspondence sent by the controller, which reads as follows:

> "*Għadha kif ċemplet is-Sinjura* [redacted] *u infurmatna li aċċess għall-garaxxijiet m'għandiex u għandha bżonn toħroġ il-karozza mill-garaxx.*
>
> *Din ir-residenta toqgħod* [redacted] *u qaltilna li mhux l-ewwel darba li ġrat din li ma jkunux avżati.*

[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).

Napprezzaw jekk tagħmlu mill-aħjar li tistgħu sabiex in-nies li għandhom il-garaxxijiet hemmhekk ikunu jistgħu jaċċessawhom bla problem ta' xejn mil-iktar fis.

Għall-iktar informazzjoni tistaw iċċemplulha fuq dan in-numru [redacted].".

3. Given that the screenshot submitted by the complainant only showed the [redacted]'s customer care as a visible recipient, and it appeared that there were three additional undisclosed recipients, the Commissioner requested the complainant to submit a copy of the complete email, including all headers and recipients. In addition, the Commissioner requested the complainant to identify the construction company to which the personal data were allegedly disclosed by the controller.

4. The complainant submitted the requested email dated the 5th August 2025, including the headers, and it was established that the controller had sent the email, containing the complainant's personal data, to the [redacted] and [redacted]. Furthermore, the complainant clarified that the "*construction company*" referred to in her complaint was in fact the [redacted]

INVESTIGATION

Request for submissions

5. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complaint, including the documentation attached thereto, and enabled the controller to submit any information which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

Submissions of the controller

6. By means of an email sent on the 15th September 2025, the controller submitted the following arguments for the Commissioner to consider during the legal analysis of the case:

    a. that the controller, as a competent authority in terms of the Data Protection (Processing of Personal Data by Competent Authorities for the purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, Subsidiary Legislation 586.08 ("**Subsidiary**

Legislation 586.08"), when faced with a case involving the prevention of an offence of a strictly criminal nature, processed the complainant's personal data and disclosed it to another public entity in line with regulation 3 and the principles set out in regulation 4 of the same subsidiary legislation; and

b. that the scope of such processing, which occurred strictly between governmental entities, was solely for the purpose of safeguarding the citizen's rights.

7. The controller was provided with the opportunity to make additional submissions regarding how it considers that the data protection principles were complied with in this case. By means of an email sent on the 25th September 2025, the controller submitted the following further arguments for the Commissioner to consider during the legal analysis of the case:

a. that since action was required to be taken directly by the [redacted] it was assumed that the complainant's identity and contact details were needed to be shared with the [redacted] in order for the matter to be effectively addressed;

b. that identifying the complainant to the [redacted] was not only necessary but crucial, as direct contact with the complainant was required in order to carry out the necessary works, from which the complainant would ultimately benefit; and

c. that the [redacted], as a separate controller, already holds and processes such personal data for every household, and that the complainant's data could have been accessed from its internal databases. Nonetheless, the sharing of the complainant's details in this case facilitated a quicker resolution and was done in the complainant's best interest.

Submissions of the complainant

8. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the complainant with the opportunity to rebut the controller's submissions. By means of an email sent on the 26th September 2025, the complainant submitted the following arguments:

a. that the complainant was never informed that her identity and contact details would be shared with the [redacted]

b. that the complainant did not provide consent for such processing of her personal data;

c. that the controller's justification that the disclosure was "*assumed necessary*" or "*in the complainant's best interest*" is not acceptable;

d. that the complainant had a reasonable expectation of confidentiality and transparency in how her personal data would be handled;

e. that the sharing of the complainant's personal data was unnecessary and disproportionate, especially since the [redacted] already holds household information; and

f. that the controller should implement appropriate safeguards and procedures to ensure that the personal data of complainants are not disclosed to third parties without the complainant's prior knowledge and consent in the future.

Final submissions of the controller

9. In accordance with the internal investigative procedure of this Office, the Commissioner provided the controller with the final opportunity to respond to the arguments made by the complainant. In this regard, by means of an email sent on the 29th September 2025, the controller submitted the following arguments for the Commissioner to consider during the legal analysis of the case:

a. that the controller's actions were proportionate, particularly in light of the complainant's request for immediate and urgent assistance. The controller maintains that the steps taken were necessary to avoid any undue delay;

b. that the controller was only able to provide the requested assistance by sharing the complainant's contact details with the [redacted]

c. that had the complainant been asked to provide explicit consent, and such consent been withheld, the complainant would have remained without access to her ramp, and thus it was indispensable for the [redacted] to communicate with the complainant directly;

d. that there was no alternative course of action available under the circumstances; and

e. that the disclosure of the complainant's personal data was justified, limited to what was strictly necessary, and ultimately in the complainant's best interest.

LEGAL ANALYSIS AND DECISION

9. As a preliminary step of the investigation, the Commissioner examined the data protection complaint lodged by the complainant on the 6th August 2025, in which the complainant alleged that the controller had unlawfully disclosed her personal data to the [redacted] and [redacted]. The Commissioner proceeded to examine the supporting documentation, which was submitted alongside the complaint, namely the email sent by the controller to the unauthorised third parties dated the 5th August 2025. The email contained the following information pertaining to the complainant: (a) name and surname; (b) email address; (c) mobile number; and (d) residential address. This information constitutes "*personal data*" within the meaning of article 4(1)[2] of the Regulation.

10. The principle of lawful processing, as set out in article 5(1)(a) of the Regulation, is one of the core data protection principles and forms part of the essence of the fundamental right to the protection of personal data. This principle requires, *inter alia*, that every data processing operation is based on a valid legal ground. In accordance with the principle of accountability under article 5(2) of the Regulation, the controller is responsible for, and must be able to demonstrate, the lawfulness of the processing activity.

11. The Court of Justice of the European Union (the "**CJEU**") held that "[a]*rticle 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 (see, to that effect, judgment of 24 November 2011, ASNEF and FECEMD, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 30 and 32)*"[3]. In a more recent judgment, the CJEU reaffirmed that "*it must be pointed out that any processing of personal data, including processing carried out by public authorities … must satisfy* ***the conditions of lawfulness set by Article 6 of the GDPR****"*[4] [emphasis has been added].

12. The processing of personal data is considered lawful when it falls within one of the six legal bases set out in article 6(1) of the Regulation, namely: (a) the data subject has given consent to the processing of personal data; (b) the processing is necessary for the performance of a

[2] Article 4(1) of the Regulation defines "*personal data*" as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".
[3] *Patrick Breyer v Bundesrepublik Deutschland* (Case C-582/14) EU:C:2016:779 [2016] para. 57.
[4] *Norra Stockholm Bygg AV v Per Nycander AB* (Case C-268/21) EU:C:2023:145 [2023] para. 29.

contract; (c) compliance with a legal obligation; (d) protection of vital interests of the data subject or another natural person; (e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (f) the pursuit of a legitimate interests by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

13. Accordingly, the Commissioner proceeded to assess whether the controller's processing of the complainant's personal data was based on at least one of these legal bases. During the course of the investigation, the Commissioner provided the controller with the opportunity to submit any information that it deemed relevant and necessary to respond to the allegation raised by the complainant. In its submissions dated the 15th September 2025, the controller stated that, as a competent authority in terms of Subsidiary Legislation 586.08, it processed the complainant's personal data in line with regulation 3 and the principles outlined in regulation 4 of the same legislation. The controller submitted that this was carried out in the context of preventing an offence of a strictly criminal nature.

Subsidiary Legislation 586.08

14. Firstly, the Commissioner notes that Subsidiary Legislation 586.08 transposes the provisions of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

15. Secondly, the Commissioner remarks that regulation 3(1) of Subsidiary Legislation 586.08 provides that *"[t]hese regulations shall apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".

16. In light of the controller's submissions of the 15th September 2025, wherein it claimed that it qualifies as a competent authority within the meaning of regulation 2 of Subsidiary Legislation 586.08, and stated that the processing of the complainant's personal data was carried out for the purpose of the prevention of a criminal offence, the Commissioner proceeded to assess and determine whether, in the circumstances of the present case, the controller falls within the scope of the definition of a "competent authority" as established under the said regulations.

17. The Commissioner notes that regulation 2 of Subsidiary Legislation 586.08 defines "competent authorities" as follows:

> *"(a) any **public authority competent for the prevention**, investigation, detection or prosecution **of criminal offences** or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and excluding the Security Service as established under the Security Service Act;*
>
> *(b) any other body or entity entrusted by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"* [emphasis has been added].

18. Accordingly, for the controller to qualify as a competent authority under Subsidiary Legislation 586.08, it must be vested with powers under national law specifically for the purpose of preventing criminal offences. In addition, regulation 38(1)(a) of Subsidiary Legislation 586.08 stipulates that the disclosure of personal data by a competent authority to public authorities is permitted only where "*the communication is strictly necessary for the performance of a task of the transferring competent authority **as provided for by law** for the purposes set out in regulation 3(1)*" [emphasis has been added]. Therefore, in the present case, the controller was required to demonstrate that the disclosure of the complainant's personal data to public authorities was strictly necessary for the performance of its designated task as provided by law, namely, the prevention of criminal offences.

19. Moreover, according to the European Commission, competent authorities as defined by Directive (EU) 2016/680 are: "*either organs of the State or private bodies, **on which the law confers special powers** beyond those which result from the normal rules applicable in relations between the individuals and/or by the possibility of exercising the power of coercion ...*"[5] [emphasis has been added].

20. After examining the submissions of the controller, the Commissioner notes that the controller did not identify or cite any specific national legislation that confers upon it the power to prevent criminal offences. In addition, the controller did not provide a satisfactory explanation

[5] European Commission, *First Report on the Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680* COM (2022) 364 final, section 2.2.1.

demonstrating that the disclosure of the complainant's personal data, who was the individual unable to exit her garage, was strictly necessary for the purpose of preventing a criminal offence. This led the Commissioner to conclude that the controller does not have any powers to perform tasks related to the prevention of criminal offences, and thus, cannot justify the disclosure of the complainant's personal data for such purpose.

Article 6(1) of the Regulation

21. As outlined in paragraph 12 of this decision, the processing of personal data is considered lawful only where it is based on one of the six legal bases set out in article 6(1) of the Regulation. In this regard, the Commissioner observed that the controller relied solely on Subsidiary Legislation 586.08 as a legal basis for its processing activity, which, for the reasons outlined above, is not applicable in the present case.

22. After carefully assessing all submissions provided by both the complainant and the controller, the Commissioner determined that the issue prompting the complainant to contact the controller concerned the obstruction of the complainant's garage by a third party, which had failed to provide any prior notice of such obstruction to the complainant. The complainant sought the controller's intervention to ensure that such third-party removed the obstruction and refrained from causing similar obstructions without notice in the future.

23. In view of these circumstances, the Commissioner is of the view that the disclosure of the complainant's personal data to the third-party company would only have been lawful if the complainant, as the data subject, had given consent to such processing pursuant to article 6(1)(a) of the Regulation. The other legal bases under article 6(1) are not applicable.

24. Furthermore, the Commissioner concludes that the disclosure of the complainant's personal data in this case was not necessary for the purpose of ensuring that the third-party refrains from obstructing garages without notice in the future, nor for securing the removal of the obstruction affecting the complainant. The controller could have effectively addressed the matter by communicating the concern to the third-party in general terms, without disclosing the complainant's name and surname, email address, mobile number, and residential address. In the Commissioner's assessment, such an approach would have been sufficient to meet the intended objective, that is, to alert the third-party to the issue while respecting the complainant's right to the protection of her personal data. In fact, although the controller argued that the processing was necessary and crucial for the resolution of the complainant's complaint, it simultaneously undermined this position by stating that *"the sharing of the complainant's details in this case ensured a **quicker** resolution"* [emphasis has been added], thereby implying

that while such disclosure may have facilitated a more expedient outcome, it was not strictly necessary for achieving the intended purpose.

25. The Commissioner noted the following from the complainant's submissions: "*I want to make it very clear that I was never informed that my identity and contact details would be passed to* [redacted]*, and I did not consent to this".* Moreover, the controller did not contest the allegation that the complainant did not give consent to such processing. In fact, in its submissions of the 29th September 2025, the controller stated: "***[h]ad explicit consent been formally requested and subsequently withheld****, the complainant would have remained without access to her ramp"* [emphasis has been added]. It is therefore evident that the processing of the complainant's personal data was not based on consent in terms of article 6(1)(a) of the Regulation.

26. The Commissioner reiterates that, in accordance with the accountability principle under Article 5(2) of the Regulation, the controller is responsible for, and must be able to demonstrate, the lawfulness of the processing activity. In this regard, the Commissioner concluded that the controller failed to demonstrate that the processing of the complainant's personal data is justified under one of the lawful bases outlined in article 6(1) of the Regulation.

On the basis of the foregoing considerations, the Commissioner is hereby deciding that the controller failed to demonstrate the lawfulness of the disclosure of the complainant's personal data to unauthorised third parties. Therefore, the Commissioner concludes that the controller infringed article 6(1) of the Regulation.

In terms of article 58(2)(b) of the Regulation, the Commissioner is hereby serving the controller with a reprimand and warned that in the event of another infringement of a similar nature, the appropriate corrective action will be taken accordingly.

By virtue of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to implement an internal policy that clearly sets out the procedure to be followed by its employees in similar cases. In particular, where the controller receives requests from data subjects who raise concerns regarding specific situations, and the resolution of such matters necessitates communication with third parties, the controller shall, prior to any disclosure of personal data to third parties, first establish whether the disclosure of the personal data of the data subjects is necessary and proportionate, and if in the affirmative seek to obtain their consent. Such consent must be obtained in full compliance with the conditions set out in articles 4(11) and 7 of the Regulation. The Data Protection Officer must be properly consulted and actively involved in the implementation of the order issued by the Commissioner.

The controller is ordered to provide the Commissioner with evidence of compliance within one (1) month from the date of service of this decision.

Ian DEGUARA (Signature)

Digitally signed by Ian DEGUARA (Signature)
Date: 2025.10.16 13:46:53 +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[6].

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"*.

[6] Further information on the appeals procedure is available on this Office's website at the following hyperlink: https://idpc.org.mt/appeals-tribunal/.