Information and Data Protection Commissioner

CDP/COMP/282/2024

[redacted]

vs

[redacted]

COMPLAINT

1. On the 5th July 2024, [redacted] (the **"complainant"**) lodged a complaint with the Information and Data Protection Commissioner (the **"Commissioner"**) pursuant to article 77(1) of the General Data Protection Regulation[1] (the **"Regulation"**) and alleged that:

    a. her right to rectification under article 16 of the Regulation had been violated by [redacted][2] (the **"controller"**). Despite her request to correct her personal data, the controller failed to update her residential address, leading to the disclosure of inaccurate health reports, compiled by [redacted] during her procedure, to third parties; and

    b. the controller had access to her personal data despite she did not have any prior relationship.

INVESTIGATION

Request for submissions

2. Pursuant to the internal investigative procedure of this Office, the Commissioner sent a copy of the complaint to the controller and provided the controller with the opportunity to make

[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.

[2] [redacted] (C [redacted]) having its registered address at [redacted]' (according to the Malta Business Registry records accessed on the 2nd April 2025).

any submissions which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

3. On the 5th August 2024, the controller submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:

   a. that the complainant needed a service from [redacted], which was requested by her;

   b. that she was asked to provide her residential address and she supplied it without hesitation, as this information was necessary for a specific purpose;

   c. that the controller had a previous residential address, which was obtained from publicly available sources, and unfortunately, the controller failed to update this with her current residential address, due to an oversight on the part of the receptionist; and

   d. that the controller did not attempt to misuse or abuse her personal data, which she provided willingly for her own needs and services.

4. The Commissioner provided the complainant with the opportunity to rebut the arguments raised by the controller. On the 14th August 2024, the complainant submitted the following counterarguments for the Commissioner to consider:

   a. that the complainant needed a gastroenterology colonoscopy and reached out to the controller via email;

   b. that the complainant was only asked for her identity card number and mobile number in an email dated the 25th May 2024. On the day of the intervention, the 12th June 2024, she noticed that the hospital's wristband displayed an old residential address of hers, a residence which she had left in December 2006. She pointed this out to the nurse, who instructed her to inform the receptionist. The complainant did so, but unfortunately, the medical reports sent electronically still showed the incorrect residential address printed at the top. The complainant subsequently emailed the controller to address this issue, yet the controller also physically sent medical histopathology reports to third parties at her old residential address;

c. that the complainant emphasises that she had never used the services of the controller before, thus the hospital should not have possessed her personal data beyond what she provided during the inquiry (email address, identity card number and mobile phone number);

d. that the complainant questioned how residential addresses can be obtained from publicly and openly available sources, as residential addresses constitute personally identifiable information that is not freely accessible to anyone. A controller's employee stated in a telephone call on the 29th June 2024 that the hospital has an agreement with Mater Dei Hospital, allowing the controller to access a patient's data upon entering the identity card number. The complainant noted that this claim is hard to believe, not only because of data protection regulations, but also because Mater Dei Hospital has had her correct and updated residential address for years;

e. that this oversight resulted in personal and sensitive information about the complainant's health falling into the hands of third parties;

f. that *"[y]ou might not have tried but you still abused of my data in the way you acquired it as well as in the way you used it despite my repeated pointing out both in person and via email. I repeat that I did not provide my address (because I wasn't asked) until I saw the need to correct the wrong address (a previous old one) that you somehow acquired"*; and

g. that the apologies offered by the receptionist, who is under the responsibility of the controller, are hardly sufficient to address the issue.

5. In line with the Office's internal complaint-handling procedure, the Commissioner provided the controller with the final opportunity to rebut the arguments made by the complainant. In this regard, by means of an email dated the 12th September 2024, the controller submitted its reply and highlighted the following salient arguments:

"a. The particulars of this client are publicly available.
b. We require these particulars and used her particulars to provide her the services that she requested from STH.
c. It was a mistake of our staff that they did not update her address.
d. This is not an abuse or misuse of her particulars, but a genuine mistake that could have happened to her other particulars".

6. The Commissioner requested the controller to confirm whether a data protection officer had been appointed, in accordance with the requirement set forth in article 37(1)(c) of the Regulation. However, no response was received. A reminder was subsequently sent, reiterating the request for this information and requesting the controller to specify the source of the publicly available information referred to in the statement: *"had a previous address which we procured from publicly and openly available sources"*.

7. In response, the controller stated *"[t]he information in question has been procured from an electoral register. This is publicly available data"*.

LEGAL ANALYSIS AND DECISION

Collection and Processing

8. The Commissioner emphasises that the protection of natural persons in relation to the processing of personal data is a fundamental right recognised by article 8 of the Charter of Fundamental Rights of the European Union. The content and structure of article 8 of the Charter helps to define the constitutive elements of this fundamental right. The first paragraph broadly states that *"[e]veryone has the right to the protection of personal data concerning him or her"*. The second paragraph specifies the content of such right by elucidating that *"[s]uch data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law"*.

9. For the purpose of investigating this complaint, the Commissioner proceeded to assess the complaint lodged by the complainant, who stated that despite notifying the controller about her outdated residential address during her visit and via several emails – a residential address which the complainant emphasised that she did not provide to the controller - her records were not updated. The controller, in its submissions, admitted that a failure by its receptionist to update the complainant's residential address led to sensitive health reports being sent to third parties at her old residential address.

10. As a preliminary step of the investigation, the Commissioner examined the definition of *'personal data'* as held in article 4(1) of the Regulation, which provides that *"**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 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" [emphasis has been added]. Additionally, the Commissioner noted that the controller processes *'data concerning health'*, which constitutes a special category of personal data in terms of article 9(1) of the Regulation. This category of personal data requires heightened protection due to the risks posed by its processing. It is therefore incumbent on the controller to ensure that the appropriate security measures are in place to specifically safeguard data concerning health.

11. During the course of the investigation, it was established that the controller processed the complainant's personal data from the Electoral Register. In fact, in its submissions, the controller argued that *"[t]he information in question has been procured from an electoral register. This is publicly available data"*. Accordingly, the Commissioner examined whether the processing of personal data conducted by the controller, particularly the use of personal data collected from the *'Electoral Register'*[3] for the purpose of providing a medical service, complies with the provisions of the Regulation.

12. Within this context, the Commissioner assessed the legal framework under the General Elections Act (Cap. 354 of the Laws of Malta), which governs the use and publication of the Electoral Register. Article 33(1) of Cap. 354 establishes that the Electoral Commission *"**shall cause a revised Electoral Register to be published in a non-searchable electronic format on its website twice a year**, that is to say, in the month of April and in the month of October"*. The purpose of such publication is further explained in article 30(3) of the Act, which provides that that the *"**Electoral Register shall be compiled in such a manner that the public may be aware of the persons who are registered as voters, and in such manner to enable identification of every voter and giving every voter the opportunity to object to the inclusion of any other voter in accordance with the provisions of this Act"*** [emphasis has been added].

13. In this regard, article 31(3) of the Cap. 354 states that *"the Electoral Register may also include against the name of each voter any other particulars which may be considered necessary for the proper identification of each voter"*. The Electoral Register, therefore, includes the following personal data: (i) name and surname of the eligible voter; (ii) residential address; and (iii) identity card number.

[3] Electoral Commission Malta, *'**Electoral Registers**'*, available at: https://electoral.gov.mt/electoral-registers

14. The Commissioner emphasises that any personal data made publicly available through the Electoral Register does not grant an automatic or absolute right to any controller to process that personal data for purposes beyond those established under Cap. 354 without a valid legal basis as required by article 6(1) of the Regulation.

Article 5(1)(a) of the Regulation

15. The Commissioner examines article 5(1)(a) of the Regulation which sets out one of the principles underpinning data processing and which provides that *"[p]ersonal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject"*.

16. The principle of lawfulness of article 5(1)(a), read together with article 6 of the Regulation, is one of the main safeguards to ensure the protection of personal data. It follows a restrictive approach whereby a controller shall only process the personal data of individuals if it is able to rely on one of the bases found under article 6 of the Regulation. The principle of lawfulness goes hand in hand with the principles of fairness and transparency in article 5(1)(a) of the Regulation. In fact, the European Data Protection Board (the **"EDPB"**) emphasises that the principles of fairness, lawfulness and transparency, all three enshrined in article 5(1)(a) of the Regulation, are three distinct but intrinsically linked and interdependent principles that every controller should respect when processing personal data[4].

17. The principle of fairness includes, *inter alia*, recognising the reasonable expectations of the data subjects, considering possible adverse consequences the processing may have on them and having regard to the relationship and potential effects of imbalance between them and the controller. In this regard, the EDPB provides that:

> *"**Fairness is an overarching principle which requires that personal data** should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be*

[4] European Data Protection Board Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on the 5th December 2022.

subject to automated individual decision-making and non-discrimination of data subjects in such processes)"[5].

18. Transparency further complements fairness by ensuring a degree of trust in the processes which will ultimately affect the data subjects. To this end, the Regulation provides sufficient guarantees in terms of articles 12 to 14, which allow the data subjects to be aware and understand *inter alia* what types of data are processed, how the data are processed, the purpose(s) of the processing and the recipients of their data.

19. The transparency principle is further articulated in recital 39 of the Regulation, which specifies that *"**it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.** The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used"* [emphasis has been added]. Against this background, the Article 29 Data Protection Working Party in its *'Guidelines on Transparency under Regulation 2016/679'* emphasises that the data subjects should know in advance what the scope and consequences of the processing entails[6].

20. As detailed in recital 60 of the Regulation, there is a strong nexus between the principle of transparency and the provision of information to data subjects. Indeed, recital 60 of the Regulation states that:

"The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the

[5] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, adopted on the 20th October 2020.
[6] Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 17/EN, WP260 rev.01 (paragraph 9).

personal data and of the consequences, where he or she does not provide such data".

The obligation to provide information to the data subjects

21. The rationale behind the principle of transparency and the related provisions, particularly articles 13 and 14 of the Regulation, is that the data subject shall be made aware, *inter alia*, of the existence of the processing activity and be provided with certain essential information about the processing activity. In its Guidelines[7], the Article 29 Working Party specified that transparency is an overarching obligation, which is necessary to enable data subjects to exercise their data protection rights in terms of articles 15 to 22 of the Regulation. In one if its judgments[8], the CJEU highlighted that the *"requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".*

22. The Article 29 Working Party additionally provides that the *"**concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles**. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR"*[9] [emphasis has been added]. Article 14 of the Regulation places an obligation upon the controller to provide the data subject with details about the processing activity where the personal data have not been obtained directly from him or her. The fact that the Regulation distinguishes between direct and indirect collection of personal data is indicative that the transparency and fairness principle should also apply to those cases where there is no direct contact between the controller and the data subject at data collection stage.

23. The wording used by the legislator in article 14(1) of the Regulation, specifically the verb *'shall provide'*, demonstrates that the controller has the obligation to proactively provide the information concerning the processing activity. The wording used does not leave room for optional disclosures, unless the controller can effectively demonstrate that one of the exemptions listed in article 14(5) applies.

---

[7] ibid 6.
[8] Judgment of the Court (Third Chamber) of 1 October 2015, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, C-201/14, ECLI:EU:C:2015:638, para. 33.
[9] ibid 6, page 5.

24. The Commissioner stresses the importance of the application of article 14 of the Regulation due to the fact that, in this specific case and in accordance with what has been confirmed by the controller, the personal data was not collected directly from the data subject, but obtained from third party sources, namely from the Electoral Register. In this regard, the controller is obliged to inform the data subjects of the details of the processing activities in the manner prescribed by the Regulation, which is a *sine qua non* for ensuring transparency, fairness and enabling the data subject to exercise control over their personal data.

25. Article 14(1) and (2) prescribes the list of information that shall be provided to the data subject. Even though the legislator distinguishes between the two sets of information, however, it is abundantly clear that all such information should be provided to the data subjects. In addition to the information which the controller is obliged to provide in terms of article 13 of the Regulation, the legislator included two (2) other types of information: (i) the categories of personal data concerned and (ii) the source from which the personal data originates.

26. The data subjects should receive a precise description of the categories of personal data processed about them, especially because the personal data would have not been obtained from them, and therefore they lack knowledge about which categories of personal data are processed[10]. Additionally, the Regulation obliges the controller to disclose the specific source of the personal data and whether it came from publicly available sources.

27. Having considered that, notwithstanding the fact that article 5(1)(a) of the Regulation encompasses the principle of lawfulness, transparency and fairness, the Article 29 Working Party[11] emphasises that *"**[t]he requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6**"* [emphasis has been added].

28. The Commissioner clarifies that any information which may be obtained from public sources does not serve as an automatic exemption to enable the controller to process the personal data pertaining to the complainant. In fact, the controller should fully comply with its data protection obligations regardless of the source from where the data originate. This is made abundantly clear in article 14 of the Regulation which imposes an obligation upon the controller to provide the data subject with information about the processing operation

[10] ibid 6, page 36.
[11] ibid 6, page 9.

where the personal data have not obtained from the data subject. In particular, article 14(2)(f) of the Regulation states that the controller should inform the data subject "*from which source the personal data originate, and if applicable,* ***whether it came from publicly accessible sources***" [emphasis has been added].

29. The Commissioner noted the complainant's submissions dated 14th August 2024, in which she stated that a controller's employee, during a telephone call on 29th June 2024, claimed the hospital had an agreement with Mater Dei Hospital allowing access to a patient's data upon entering their identity card number. Based on the investigation's findings, the Commissioner concluded that the controller had not obtained the **complainant**'s personal data directly from her, or from Mater Dei Hospital, but rather from the Electoral Register.

30. Consequently, in accordance with article 14 of the Regulation, the controller was required to inform the complainant about the source form where her personal data were collected. This should have been done within the statutory deadline set out in the Regulation[12]. During the investigation the Commissioner established that the controller failed to comply with this legal requirement.

The Rectification Request

31. The Commissioner analysed the complainant's submissions, in which she alleged that she had used the controller's services for the first time on the 12th June 2024, providing only her name, mobile number and identity card number. She insisted that despite sharing limited data, the controller somehow retrieved an old postal residential address where she had lived until December 2006. She first noticed the issue when she saw the hospital wristband displaying her previous residential address. After informing the receptionist of the error, she was assured that the residential address had been updated. However, on the 24th June 2024, the complainant received a soft copy of her histopathology report, which still displayed the incorrect residential address. Thus, on the 25th June 2024, she contacted the controller again by means of two (2) emails to highlight that her residential address was not updated or rectified. The complainant later discovered that a hard copy of the histopathology report had been sent to her previous residential address and was therefore received by the current resident, who informed her accordingly. As part of her substantial evidence, the complainant provided a copy of the letter containing the incorrect residential address.

[12] Article 14(3)(a) of the Regulation imposes an obligation upon the controller to provide information within a reasonable period after obtaining the personal data, but at least within one (1) month after having obtained it.

32. In this regard, the Commissioner assessed the right to rectification set out under article 16 of the Regulation, which provides that the "*data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*".

33. The Commissioner emphasises that the right to rectification is a key aspect of the fundamental right to data protection, which is recognised in article 8(2) of the Charter of Fundamental Rights of the European Union. Within this context, article 16 of the Regulation provides for the right to rectify inaccurate data and the right to complete incomplete data. Therefore, the controller should not ignore the fact that it is responsible for keeping the data up-to-date, and thus, the controller should take every reasonable step to ensure respect of the accuracy principle as set forth in article 5(1)(d) of the Regulation.

34. The principle of accuracy requires the controller to have "*regard to the purposes for which* [data] *are processed*", which means that the data must be accurate enough for the specified purpose of the processing conducted by the controller. The case-law of the Court of Justice of the European Union (the "**CJEU**") has determined that the principle of accuracy is purpose and context-dependent, and therefore, the data must be accurate enough for the specified purpose of the processing. In Peter Nowak case, the CJEU explored the principle of accuracy in the context of the previous data protection framework, which continues to be relevant under the current legislation:

> "*It is apparent from Article 6(1)(d) of Directive 95/46* ***that the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected****. That purpose consists, as far as the answers submitted by an examination candidate are concerned, in being able to evaluate the level of knowledge and competence of that candidate at the time of the examination.* [emphasis has been added]"[13].

35. Therefore, in the present case, the principle of accuracy, as confirmed by the interpretation of the CJEU, provides that if the processing of the residential address is necessary for the

[13] Case C-434/16, *'Peter Nowak vs Data Protection Commissioner'*, Judgment of the Court (Second Chamber) of 20 December 2017, paragraph 53.

controller to achieve the purpose of the processing, it remains the responsibility of the controller to take those reasonable steps to ensure that the data are accurate throughout the whole cycle of the data. This is also in accordance with the overarching principle of data accountability as set forth in article 5(2) of the Regulation, which provides that not only the personal data are processed in an accurate manner, but also that the controller must be responsible for and be able to demonstrate compliance with the principle of data accuracy.

36. After assessing the case, the Commissioner determined that the controller failed to take reasonable steps to ensure that the complainant's personal data were accurate. The CJEU had confirmed that it is the controller who shall bear the responsibility to ensure compliance with its obligations regarding the quality of the data. The CJEU stated that *"the principles of protection must be reflected, on the one hand,* ***in the obligations imposed on persons responsible for processing, in particular regarding data quality***"[14] [emphasis has been added]. Within this context, *'data quality'* refers to the requirement incumbent upon the controller to ensure that the data processed by the controller are kept accurate, complete and up to date.

Failure to designate a Data Protection Officer

37. Hospitals process vast amounts of personal data, including data concerning health, which necessitates heightened compliance with the Regulation. Article 37(1)(c) of the Regulation requires controllers to appoint a data protection officer where *"the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9"*. *'Data concerning health'* is defined in article 4(15) of the Regulation as *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about this or her health status"*. Therefore, given that the controller's core business activities inherently involve the large-scale processing of such data, appointing a data protection officer is a mandatory requirement under the Regulation.

38. During the course of the investigation, the Commissioner sought to confirm whether the controller had appointed a data protection officer in accordance with articles 37 to 39 of the Regulation. Notwithstanding requests for clarification, the controller failed to respond. In the light of the controller's obligation, pursuant to article 37(7) of the Regulation, to

[14] Court of Justice of the European Union, *'College van burgemeester en wethouders van Rotterdam vs M.E.E. Rijkeboer'* (Case C-553/07), decided on the 7th May 2009, paragraph 48.

communicate the data protection officer details to the Commissioner upon their designation, the Commissioner proceeded to review its internal records to determine if any information had been submitted by the controller in this respect. The Commissioner confirms that no record exists.

39. The role of the data protection officer is central to ensuring compliance with the Regulation, particularly when processing special categories of data. Article 39 of the Regulation outlines the **data protection officer**'s tasks, which include *"to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions"*, as well as *"to monitor compliance with this Regulation"*. The controller's failure to designate a data protection officer calls into question its ability to meet these obligations and maintain the necessary safeguards to protect data subjects' rights effectively.

40. The importance of appointing a data protection officer is also underscored in recital 97 of the Regulation, which highlights that *"**[s]uch** data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks **in an independent manner**"*. Furthermore, article 32(1) of the Regulation imposes a requirement on controllers to *"**implement appropriate technical and organisational** measures to ensure a level of security appropriate to the risk*" **and the** data protection officer plays a pivotal role in guiding these measures, particularly in contexts where the processing of special categories of personal data entails significant risks to individuals' rights and freedoms.

Summary of Findings

41.

	Article of the Regulation	**Findings**
1	Article 5(1)(a), article 6(1) and article 14 of the Regulation	The controller collected and processed the **complainant's personal** data from the Electoral Register without a legal basis and without informing the complainant, *inter alia*, from which source her personal data originate, in particular, that it came from a publicly accessible source.

2	Article 16(1) and article 5(1)(d) of the Regulation	The controller failed to rectify the complainant's personal data, despite being notified multiple times and failed to take reasonable steps to ensure that the personal data being processed is accurate and up to date, as required under the accuracy principle enshrined in article 5(1)(d) of the Regulation.
3	Article 37(1)(c) of the Regulation	The controller is a healthcare provider that processes special category personal data (health data) on a large scale, and therefore, the designation of a data protection officer is mandatory under article 37(1)(c) of the Regulation.

Exercise of Corrective Powers

42. The Commissioner takes into account the toolset of corrective powers at his disposal where it results that the processing operation infringes the provisions of the Regulation. These include, *inter alia*, the power to impose an effective, proportionate and dissuasive administrative fine pursuant to the list of circumstances that refer to the features of the infringement.

43. The Commissioner notes that article 58(2) of the Regulation outlines the corrective powers that supervisory authorities may exercise in cases of non-compliance by a controller or processor. In determining whether to exercise these powers, recital 129 of the Regulation provides the following guidance: "*...**each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case**".*

44. Having carefully considered the infringements identified in this decision, the Commissioner has decided to exercise certain corrective powers under article 58(2) of the Regulation. In this regard, the Commissioner has determined that the appropriate corrective powers to address these infringements are:

    a. article 58(2)(b) of the Regulation to issue a reprimand to the controller for its infringements of the Regulation identified in this decision;

b. article 58(2)(d) of the Regulation to order the controller to bring its processing into compliance with the Regulation; and

c. article 58(2)(i) of the Regulation to impose administrative fines, pursuant to article 83 of the Regulation, in response to the controller's infringements identified in this decision.

Imposition of a reprimand

45. Article 58(2)(b) of the Regulation provides that a supervisory authority shall have the power *"to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"*.

46. The Commissioner has decided to issue a reprimand to the controller for the infringements identified in this decision, aiming to deter non-compliance with the Regulation.

47. The infringements relate to the processing of incorrect personal data obtained from a publicly available source, demonstrating a failure to comply with several substantive provisions of the Regulation, including an infringement of the principle outlined in article 5(1)(a) of the Regulation, a failure to respect data subjects' rights and the failure to designate a data protection officer despite processing large volumes of special categories of personal data. Moreover, the controller should not ignore the fact that it is responsible for keeping personal data up to date and must take every reasonable step to ensure compliance with the accuracy principle, as required under article 5(1)(d) of the Regulation. The failure to rectify inaccurate data in a timely manner led to unauthorised disclosure of personal data. Given the seriousness of these breaches, reprimands are appropriate in respect of such non-compliance, to formally recognise the serious nature of the infringements and to dissuade such non-compliance.

48. The reprimand is necessary and alongside the other corrective measures imposed in this decision. The Commissioner considers it appropriate to issue this reprimand to the controller to deter future similar non-compliance actions. A reprimand is proportionate in the circumstances where it does not exceed what is required to enforce compliance with the Regulation, taking into account the serious nature of the infringements and the potential for harm to data subjects.

Order to bring processing into compliance

49. Article 58(2)(d) of the Regulation provides that a supervisory authority shall have the power *"to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period"*.

50. The Commissioner considers that, under article 58(2)(d) of the Regulation, an order should be imposed requiring the controller to bring processing into compliance by taking the following actions:

    a. to comply with the request made by the complainant and rectify her personal data, pursuant to article 16 of the Regulation;

    b. to delete the personal data of other data subjects obtained from the Electoral Register; and

    c. to designate a data protection officer pursuant to article 37 of the Regulation.

51. In light of the non-compliance identified in this decision, the Commissioner considers the order to be both necessary and proportionate, representing the minimum action required to ensure that the controller achieves full compliance in the future. While the order imposes specific remedial obligations on the controller, the reprimand serves to formally acknowledge the seriousness of the infringements, and together, these measures are deemed essential and proportionate in addressing the non-compliance outlined in this decision.

52. Accordingly, the controller is required to comply with this order **within twenty (20) days from the date of service of this decision**, and within the same period, confirm the actions taken to align its processing activities with the Regulation.

Administrative fines

53. Article 58(2)(i) of the Regulation provides that a supervisory authority shall have the power *"to impose an administrative fine pursuant to Article 83, **in addition to,** or instead of measures referred to in this paragraph, depending on the circumstances of each individual case"* [emphasis has been added]. This makes it clear that the Commissioner has the power to impose administrative fines either in addition to, or as an alternative to the other corrective powers specified in article 58(2) of the Regulation.

54. Article 83(1) of the Regulation provides that *"[e]ach supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*.

55. The Commissioner therefore proceeded to examine article 83(2) of the Regulation, which provides certain criteria in deciding whether to impose an administrative fine and on the amount of the administrative fine in each individual case.

56. In applying the factors under article 83(2)(a) to (k) of the Regulation to the infringements, the Commissioner has analysed them collectively where appropriate. However, the Commissioner has considered every infringement separately when deciding whether to impose an administrative fine in respect of each infringement. Each decision is made separately, without prejudice to any factors arising from other infringements. For clarity, the decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine, where applicable, is independent and specific to the circumstances of each infringement.

Article 83(2)(a) of the Regulation

57. Due regard was given to article 83(2)(a) of the Regulation, which refers to *"**the nature**, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of **damage suffered by them**"*.

58. The Commissioner determines that the core issue in this case is the lack of a lawful basis for the processing of the complainant's personal data. The Commissioner highlights that every processing operation which falls within the meaning of article 4(2) of the Regulation must have a legal basis 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 controller shall be responsible for, and be able to demonstrate that the disclosure of the video recording to a third party is indeed lawful.

59. 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 (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)"2. 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**"*[15] [emphasis has been added].

60. It therefore follows that the processing of personal data is deemed lawful if it comes within 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 was required to demonstrate that the collection and use of the complainant's personal data, more specifically, obtaining the data from the Electoral Register and processing it for the purpose of providing a medical service to the complainant, was based on at least one of these legal bases. However, during the course of the investigation, the controller failed to identify any of these legal grounds to justify the lawfulness of the processing.

61. Moreover, insofar as the nature of the infringement is concerned, the Commissioner observed that the controller failed to give the right of the complainant its full broadest effect. The rights of the data subjects as set forth in Chapter III of the Regulation are the fulcrum and the basis of the law and their role is crucial to give the data subjects control over their personal data. It is indeed the intention of the legislator to sanction any infringement of the data subjects' rights in an appropriate and effective manner, considering that these rights constitute the fundamental basis on the strength of which protection and control are afforded to data subjects with regard to the processing of their personal data.

62. The investigation conducted by the Commissioner revealed that despite multiple notifications from the complainant, both in person and via email, regarding the rectification of an old address which the controller did not collect directly from the complainant but retrieved from an electoral register, the controller continued to process and use the incorrect personal data. The Commissioner considers this infringement to be a serious one, particularly given that the failure to accede to the complainant's right to rectification resulted in sensitive health-related personal data, including histopathology reports, being sent to an incorrect and outdated address, thereby exposing the complainant's private medical information to unauthorised third parties. This failure not only demonstrated negligence in

[15] Case C-268/21, *Norra Stockholm Bygg AV v Per Nycander AB*, decided on the 2nd March 2023.

ensuring the accuracy of the personal data, as required under article 5(1)(d) of the Regulation, but also highlighted the absence of a lawful legal basis for processing data that was inaccurate and outdated.

63. Additionally, the Commissioner examined the duration of the infringement, which significantly contributes to the gravity of the infringement. The complainant highlighted that the postal address used by the controller was an old residence she had vacated in December 2006, nearly two decades prior to the events in question. This suggests that the controller had retained outdated and irrelevant personal data for an excessive period without any apparent effort to ensure its accuracy.

Article 83(2)(b) of the Regulation

64. Article 83(2)(b) of the Regulation provides that one of the general conditions is the "*intentional or negligent character of the infringement*". The Commissioner examined whether the character of the infringement committed by the controller was intentional or negligent. The European Data Protection Board's (the **"EDPB"**) *'Guidelines on the application and setting of administrative fines'*[16] provide that *"**in general, intent includes** both knowledge and wilfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law"*.

65. On the basis of the facts gathered during the course of the investigation, the Commissioner established that there is no evidence that the controller had acted intentionally, although its actions, particularly the controller's repeated failure to accede to the complainant's request to have her residential address rectified and its reliance on data obtained from the Electoral Register to populate and maintain patient records, demonstrate serious lack of diligence.

Article 83(2)(c) of the Regulation

66. The Commissioner examined article 83(2)(c) of the Regulation, which addresses *"**any** action taken by the controller or processor to mitigate the damage suffered by data subjects"*.

[16] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, adopted on the 3rd October 2017.

67. During the course of the investigation, the Commissioner found that the controller not only failed to prevent the unauthorised disclosure of the complainant's medical results but also neglected to act promptly when informed about the matter. This lack of adequate internal controls for real-time correction of data inaccuracies revealed systemic deficiencies in the controller's data governance practices.

68. Health data, classified as a special category of personal data under article 9(1) of the Regulation, demands a particularly high standard of diligence in its handling. As a healthcare provider processing sensitive health data on a large scale, the controller bears a heightened responsibility to implement robust compliance measures to protect the rights and freedoms of data subjects. However, the evidence highlights significant organisational failures in fulfilling these obligations.

69. One of the most significant indicators of the controller's lack of responsibility is its failure to designate a data protection officer, as required under article 37(1)(c) of the Regulation. This provision mandates the appointment of a data protection officer when *"the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9"*. Given the controller's role and the volume of health data it processes, designating a data protection officer is mandatory.

Article 83(2)(d) of the Regulation

70. The Commissioner examined article 83(2)(d) of the Regulation which relates to *"the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 to 32"*. Upon review, the Commissioner determined that this provision is not applicable in this case.

Article 83(2)(e) of the Regulation

71. Article 83(2)(e) of the Regulation provides for *"any relevant previous infringements by the controller or processor"*. In this case, The Commissioner confirmed that the controller did not have any relevant prior infringements.

Article 83(2)(f) of the Regulation

72. Article 83(2)(f) of the Regulation stipulates that the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse

effects of the infringement may be taken into account by the supervisory authority in deciding whether to impose an administrative fine and on the amount of the fine.

73. The Commissioner's initial request for submissions sent on the 10th July 2024, went unanswered until a reminder was issued on the 2nd August 2024, prompting the controller's reply on the 5th August 2024. The lack of cooperation became evident following the Commissioner's request for clarification regarding the data protection officer on the 4th November 2024. The controller ignored this request, prompting another reminder on the 9th December 2024, which reiterated the need for information on the data protection officer and clarification on the source of the publicly available information. While the controller replied on the same day, the response addressed only one aspect and completely omitted the data protection officer query - a critical factor in assessing compliance with articles 37 to 39 of the Regulation.

Article 83(2)(g) of the Regulation

74. In assessing the categories of personal data affected by the infringement, the Commissioner established that these included basic biographical information of the complainant - her name and surname – her residential address and data concerning her health, which specifically included the medical result of her histopathology. These data were disclosed to unauthorised third parties.

75. The Regulation provides heightened protection to the processing of special categories of personal data due to the significant risks in relation to the protection of the data subjects' rights and freedoms, particularly the irreversible and long-term consequences, which may occur as a result of the processing activity[17].

76. By comparing these categories to the definition of *'personal data'*[18] and to the criteria required to determine whether a natural person is identifiable or otherwise[19], the

[17] Recital 51 of the Regulation: *"**Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms**".*

[18] Article 4(1) of the Regulation defines personal data as *"**any information relating to an identified or identifiable natural person**".*

[19] Pursuant to recital 26 of the Regulation *"**[...] to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments [...]**".*

Commissioner concluded that the data subject was indeed identified. This resulted in a significant risk to the rights and freedoms in the context of the protection of her personal data in view of potential malicious use by third parties.

Article 83(2)(h) of the Regulation

77. After assessing article 83(2)(h) of the Regulation, the Commissioner noted that the infringement became known to him as a result of a complaint lodged by the affected data subject pursuant to article 77(1) of the Regulation.

Article 83(2)(i) of the Regulation

78. The Commissioner noted article 83(2)(i) of the Regulation stating that *"where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures"*. In this case, no corrective measures have previously been ordered against the controller concerning the subject matter of the decision. As a result, this factor is neither aggravating nor mitigating in these circumstances.

Article 83(2)(j) of the Regulation

79. The Commissioner also considered article 83(2)(j) of the Regulation, which provides for adherence to approved codes of conduct under article 40 or approved certification mechanisms under article 42 of the Regulation. These considerations do not apply in this case.

Imposition of an administrative fine

80. In deciding whether to impose an administrative fine in respect of each infringement, the Commissioner had regard to the factors outlined in article 83(2)(a) to (j) of the Regulation cumulatively. However, each infringement has been assessed separately when applying those factors, deciding whether to impose a fine and determining its amount. The Commissioner has also had regard to the effect of a reprimand and order to bring processing into compliance, ensuring that they contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements.

81. The Commissioner considers that a reprimand is of significant value in dissuading future non-compliance, as a formal recognition of the controller's identified infringements. The order to bring processing into compliance should result in the controller's immediate action to remedy the identified infringements. However, the Commissioner considers that these measures alone are not sufficient in the circumstances to ensure compliance, and therefore, he finds that imposing three (3) administrative fines is appropriate, necessary and proportionate to ensure compliance with the provisions of the Regulation.

82. The infringed articles include a fundamental principle of the Regulation under article 5(1)(a) of the Regulation, the requirement for processing to be conducted on a lawful basis under article 6(1) of the Regulation, the obligation to provide clear and accurate information about the source of personal data under article 14(2)(f) of the Regulation, and the obligation to rectify inaccurate data without undue delay under article 16 of the Regulation. Additionally, the controller failed to comply with article 37(1)(c) of the Regulation, which placed an obligation on the controller to designate a data protection officer due to its large-scale processing of data concerning health. The Commissioner considers that administrative fines are appropriate, necessary and proportionate to dissuade future non-compliance by the controller.

83. In reaching the conclusion that the administrative fines are necessary, the Commissioner had particular regard to the nature, gravity and duration of the infringements under article 83(2)(a) of the Regulation, the fact that it did not result that the controller acted negligently under article 83(2)(b) of the Regulation but rather knowingly failed to rectify inaccurate personal data despite multiple notifications, the lack of any action taken by the controller to mitigate the damage suffered by the complainant under article 83(2)(c) of the Regulation and the categories of personal data affected, including special categories of data personal under article 83(2)(g) of the Regulation, specifically health data, which requires the highest level of protection. The Commissioner has balanced these factors with the mitigating factors identified above, while also considering the toolbox of corrective powers available under article 58(2) of the Regulation.

Article 83(3) of the Regulation

84. Having completed the Commissioner's assessment of whether or not to impose a fine and its amount, it is necessary to consider article 83(3) of the Regulation to determine if there are any factors that might require the adjustment of the fines. The Commissioner noted article 83(3) of the Regulation providing that *"[i]f a controller or processor intentionally or*

negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for ***the gravest infringement****"* [emphasis has been added].

85. In this case, the identified infringements arise from linked processing operations, requiring the Commissioner to assess whether the total fine should be capped based on the gravest infringement. The infringements of article 5(1)(a), article 6(1), article 16 and article 14(2)(f) of the Regulation fall under article 83(5) of the Regulation, which allow for fines of up to **€20 million or 4% of total worldwide annual turnover, whichever is higher.** The infringement of article 37(1) of the Regulation falls under article 83(4) of the Regulation, which has a lower maximum fine of **€10 million or 2% of global turnover.** Since the most serious infringements fall under article 83(5) of the Regulation, the total administrative fine must not exceed the maximum limit applicable to those violations.

Categorisation of the infringements

86. As noted in the EDPB *'Guidelines 04/2022 on the calculation of administrative fines under the GDPR'*[20] (**"Guidelines 04/2022"**), article 83(4) to article (6) of the Regulation establish different levels of infringement severity. Guidelines 04/2022 state that *"[w]ith this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be".*

Seriousness of the infringement pursuant to articles 83(2)(a), (b) and (g) of the Regulation

87. The EDBP's Guidelines 04/2022 state that the factors assessed under article 83(2)(a), article 83(2)(b) and article 83(2)(g) of the Regulation determine the seriousness of an infringement[21]. It outlines that *"[t]he assessment of the factors above determines the seriousness of the infringement as a whole. This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole"*[22].

[20] European Data Protection Board, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, (Version 2.1) adopted on the 24th May 2023.
[21] Ibid, page 17.
[22] Ibid, page 21.

88. The Commissioner considered these factors as a whole and noted that the infringements are of a high level of seriousness. Under article 83(2)(a) of the Regulation, the infringements were found to be of a serious nature due to the violations of fundamental principles, including fairness, lawfulness and transparency. The infringements were also found to have been of moderate duration, as the controller failed to rectify inaccurate personal data despite multiple notifications. The processing affected special categories of personal data (health data), which, by its nature, poses a heightened risk to the fundamental rights and freedoms of data subjects, as assessed under article 83(2)(g) of the Regulation. Additionally, the controller acted with lack of diligence, as it continued to process inaccurate personal data and provided misleading assurances regarding rectification, as assessed under article 83(2)(b) of the Regulation. Therefore, balancing these factors, the Commissioner considers that the infringements were of medium seriousness.

Imposing an effective, dissuasive and proportionate fine

89. Article 83(1) of the Regulation requires fines to be effective, proportionate and dissuasive in each individual case. As the Guidelines 04/2022 also say that this *"does not dismiss a supervisory authority from the responsibility to carry out a review of effectiveness, dissuasiveness and proportionality at the end of the calculation"*[23]. Therefore, article 83(1) of the Regulation will be reconsidered at the conclusion of this calculation.

Aggravating and mitigating circumstances

90. Article 83(2)(a), article 83(2)(b) and article 83(2)(g) of the Regulation were considered above. This section examines the aggravating or mitigating impact of the remaining criteria in article 83(2) of the Regulation. Regarding article 83(2)(c) of the Regulation, the controller failed to prevent the unauthorised disclosure of the complainant's health data and did not act promptly when informed. The investigation revealed systemic deficiencies in data governance, including inadequate controls for correcting inaccuracies. As a healthcare provider processing large-scale sensitive data, the controller had a heightened duty to protect data subjects but failed to meet this obligation. Notably, it also failed to appoint a data protection officer as required under article 37(1)(c) of the Regulation, despite its legal obligation to do so.

[23] Ibid, page 24.

91. In relation to article 83(2)(e) of the Regulation, the Commissioner noted that the controller had no prior relevant infringements, considering this factor neither mitigating nor aggravating. Under article 83(2)(f) of the Regulation, the controller cooperated with the Commissioner. The infringement came to the Commissioner's attention via a data subject's complaint, as per article 83(2)(h) of the Regulation. Finally, the Commissioner deems articles 83(2)(d), (i) and (j) of the Regulation to be neither mitigating nor aggravating.

92. For the reasons outlined above and with particular regard to article 83(2) of the Regulation and the Guidelines 04/2022[24], the Commissioner has decided to impose the following administrative fines on the controller:

a. **twelve thousand and five hundred Euro (€12,500)** for the infringement of article 5(1)(a), article 6(1) and article 14(2)(f) of the Regulation;

b. **five thousand Euro (€5,000)** for the infringement of article 16 of the Regulation; and

c. **two thousand and five hundred Euro (€2,500)** for the infringement of article 37(1)(c) of the Regulation.

Article 83(1) of the Regulation: Effectiveness, proportionality and dissuasiveness

a. Effectiveness

93. The Commissioner believes that for a fine to be *'effective'*, it must be substantial enough to influence the controller or processor, ensuring that compliance with the Regulation becomes a key factor in governance and high-level decision-making. In this case, the infringements concern fundamental principles of the Regulation, particularly fairness and transparency, which safeguard data subjects' control over their personal data, uphold their right to rectification and prevent unlawful or misleading processing. The unauthorised disclosure of special categories of personal data further amplifies the risks to the complainant's rights and freedoms. Thus, considering these factors, the Commissioner deems the imposed fines effective, requiring no further adjustment.

b. Dissuasiveness

[24] Ibid

94. For a fine to be *'dissuasive'*, it must deter both the specific controller or processor involved and others engaging in similar processing operations from repeating the misconduct. The Commissioner considers the imposed fines sufficient to achieve this deterrent effect. Each infringement is serious in nature and gravity, as outlined in article 83(2)(a) of the Regulation. Violations of fundamental principles of the Regulation, including fairness, lawfulness and transparency demand strong corrective measures. The Commissioner emphasises that non-compliance with these principles must be firmly addressed to uphold data subjects' rights and reinforce the importance of adherence. Therefore, the imposition of administrative fines is both appropriate and necessary to prevent future non-compliance.

95. The controller's failure to ensure transparency, rectify errors despite multiple notifications and unlawfully rely on publicly accessible sources without informing data subjects demonstrates a serious disregard for the obligations emanating from the Regulation. This negligence underscores the necessity of administrative fines to ensure that the controller takes its responsibilities seriously and implements the necessary corrective measures.

96. The Commissioner considers that the imposition of administrative fines will encourage the controller and other similar entities to take appropriate action to prevent further infringements. While the Commissioner acknowledges the controller's lack of prior infringements as a minor mitigating factor, it does not lessen the severity of the current violations. Given the negligent character of the infringements and the controller's failure to uphold its obligations, the Commissioner considers that the imposition of dissuasive administrative fines is necessary to ensure future compliance.

c. Proportionality

97. *'Proportionality'* is a fundamental principle of EU law, requiring that any measure pursues a legitimate objective, is appropriate to achieve that objective and does not exceed what is necessary. The objectives of the administrative fines in this case are to re-establish compliance with the provision of the Regulation and to sanction the controller's infringements.

98. The Commissioner considered the nature, gravity and duration of the infringements, he deems the administrative fines proportionate to ensuring compliance. The controller's failure to lawfully process personal data, ensure transparency, rectify inaccurate data and appoint a data protection officer constitutes a serious violation of the core principles. In light of this, the Commissioner finds the administrative fines appropriate to address the

controller's infringement and promote future compliance. The administrative fines do not exceed what is necessary to enforce compliance with the identified infringements in this decision.

SUMMARY OF ENVISAGED ACTION

In summary and on the basis of the foregoing considerations, the Commissioner is hereby exercising on the controller the following corrective powers under article 58(2) of the Regulation:

i. **a reprimand pursuant to article 58(2)(b) of the Regulation regarding the infringements identified in this decision, particularly:**

   a. **the unlawful processing of personal data obtained from a publicly available source, demonstrating non-compliance with the principle of lawfulness as set forth in article 5(1)(a) and article 6(1) of the Regulation, and a failure to ensure fair and transparent processing in terms of the requirements set forth in article 14 of the Regulation;**

   b. **the failure to rectify inaccurate data in a timely manner and failure to take every reasonable step to ensure compliance with the accuracy principle, as required under article 5(1)(d) and article 16 of the Regulation; and**

   c. **the failure to designate a data protection officer pursuant to article 37(1)(c) of the Regulation, despite being a healthcare provider processing large-scale special categories of data.**

ii. **an order pursuant to article 58(2)(d) of the Regulation, requiring the controller to bring processing into compliance by taking the following actions:**

   a. **ensure rectification of personal data in compliance with article 16 of the Regulation, by amending the complainant's personal data without undue delay;**

   b. **erase the personal data of all the other data subjects obtained from the Electoral Register; and**

   c. **designate a data protection officer in terms of article 37 of the Regulation.**

The aforementioned orders shall be complied without undue delay and by no later than twenty (20) days from the date of service of this legally-binding decision and confirmation of the action taken shall be notified to the Commissioner immediately thereafter.

iii. **the imposition of three (3) effective, proportionate and dissuasive administrative fines pursuant to article 58(2)(i) of the Regulation, as follows:**

a. **twelve thousand and five hundred Euro (€12,500) for infringing article 5(1)(a), article 6(1) and article 14 of the Regulation;**

b. **five thousand Euro (€5,000) for infringing article 16 of the Regulation; and**

c. **two thousand five hundred Euro (€2,500) for infringing article 37(1)(c) of the Regulation.**

The total amount of the fine shall be paid within twenty (20) days from the date of service of this legally-binding decision.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2025.04.02 15:35:28 +02'00'

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.