Information and Data Protection Commissioner

CDP/COMP/194/2023

[redacted]

vs

[redacted]

COMPLAINT

1. On the 3rd February 2023, [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**"), alleging that [redacted] (the "**controller**") requested a copy of the test results for the purpose of processing a refund for a health claim. The complainant, a holder of a health insurance policy with [redacted] deemed the request of the controller to be excessive and goes contrary to the provisions of the Regulation.

2. The complainant submitted a copy of the email correspondence exchanged between the parties, wherein the controller requested the complainant on the 17th January 2023 to "*provide us Lab Result reports to processes* [sic] *your claim further*" and "[a]*ccording to the terms and conditions we need copy of result reports to processes* [sic] *your claim*". The controller referred to clause 6.1 of the terms and conditions, which reads as follows:

"*6.1 Out-patient treatment:*

[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.

Always visit your general practitioner for each new medical condition. The GP will complete part 5A of your claim form. If you need further treatment, the specialist will complete part 5B of the claim form. All specialist consultations must be GP referred. We will only make an exception for consultations with a gynaecologist or paediatrician for children up to 10 years of age.

Send us the completed claim form within two months of the date of your first treatment, with original receipts for consultations and any tests. We will also need a copy of your test results."

INVESTIGATION

3. On the 24th February 2023, pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions on this complaint, including any other information which it deemed relevant to submit in connection with the allegation raised by the complainant.

4. On the 16th March 2023, the controller submitted the following arguments for the Commissioner to consider during the legal analysis of this case:

   a. that the controller received the Claim Form on the 9th January 2023 which depicted a specialist medical visit and the complainant requested a refund of the test done;

   b. that the consultant's report indicated the reason to be '*pelvic pain*' on the Claim Form, however, the underlying medical cause was not clearly identified from the information provided, and as a result, this reason alone is not sufficient to determine the underlying medical cause;

   c. that, therefore, the controller requested the complainant to provide it with a copy of the test results since pelvic pain may lead to various underlying causes which are not covered by the health insurance policy;

   d. that the controller does not normally request additional evidence when processing a health claim, however, in some instances, when the controller does not have enough information to assess the risk properly, such as the information provided in this case, it asks for copies of the test results;

e. that such requests are a normal market practice which assist insurers to verify the validity of the claim, and that a clause under its terms and conditions[2] states that more information may be requested on demand;

f. that the information requested in this case is solely to ascertain the eligibility of the claim, without which the controller will not be able to conclude its investigation and settle the claim, and that, when the controller is certain that the claim for the medical treatment is covered under its policy, it will reimburse the complainant accordingly; and

g. that, in a previous case and prior claim, the same complainant had submitted a copy of the test results on his own free will without the results being requested by the controller.

5. Following receipt of the *supra* submissions, the Commissioner requested further clarifications from the controller due to conflicting versions held in its submissions and the Health Insurance Policy. The controller stated that more information may be requested on demand as per its terms and conditions, however, this does not seem to reflect the wording of clause 6.1 of the Health Policy, which states that "*we will also need a copy of your test results*"[3].

6. The controller clarified that "[redacted] *do have specifically written in their T&Cs that a copy of any tests done should be submitted to* [redacted] *as was evidenced in the attachment. It is a market practice that whenever an insurer is unclear about a claim, more information/clarification is required. A Fact which is not clearly specified in our T&Cs and it is our intention to match the T&Cs with our current procedures*".

7. On the 27th March 2023, the Commissioner provided the complainant with the opportunity to rebut the arguments made by the controller, and by means of an email dated the 1st April 2023, the complainant submitted the following principal arguments;

a. that the policy makes it amply clear that the test results are always required, as opposed to the controller's claim that the results are only requested in certain situations, and that therefore the policy goes against the principles of the Regulation;

b. that the controller never clarified why the test results were needed, but merely requested medical results without explaining the reason for such a request, and this despite the

[2] The controller provided a copy of the Health Insurance Policy.
[3] Clause 6.1 'Out-patient treatment': "*Send us the completed claim form within two months of the date of your first treatment, with original receipts for consultations and any tests. We will also need a copy of your test results*".

lengthy communication between the parties prior to the lodging of the complaint with the Commissioner;

c. that the controller always requested the documentation in order to process the claim, and when asked why, the controller relied on the terms and conditions as found in the policy, which, according to the complainant, shows that their practice is to always ask for the medical test results;

d. that Section 5 – Part B of the Health Insurance Claim Form only required the complainant to list the symptoms or the medical condition (in this case, it was '*pelvic pain*'), and there is no other section of the Claim Form which requires the claimant or medical health professional to list the underlying cause of the symptoms;

e. that if the Claim Form is inadequate for the controller's processing purposes and creates ambiguity, it is the controller's responsibility to take the necessary steps and modify the Claim Form, rather than immethodically ask for the complete medical test results and process any information which it wants; and

f. that the fact that the complainant sent in the medical results in a previous separate claim should not make any difference, and the reason he submitted the results in that instance is due to his unawareness of the provisions of the Regulation.

8. The controller was requested to rebut the arguments made by the complainant. By means of an email dated the 17th April 2023, the controller submitted the following arguments:

a. that it had provided sufficient and justified reasons for requesting the medical test results in its prior communication with the complainant and before the lodging of the complaint;

b. that the complainant may solely be seeking redress in order to avoid submitting the test results, which potentially might show that the underlying cause is not covered by the insurance policy;

c. that the fact that the complainant had previously submitted the test results without issue, combined with the complainant's continuous and persistent refusal to submit the current medical results increases the controller's suspicions about the present claim; and

d. that since the complainant ascertained in his submissions that he '*has nothing to hide and have no problems submitting the test result*', therefore there should be no issue with submitting the same.

LEGAL ANALYSIS AND DECISION

General Considerations

9. After assessing the complaint lodged in terms of article 77(1) of the Regulation, the Commissioner sought to determine: (i) whether the request submitted by the controller for a copy of the medical test results is adequate and relevant for the purpose of attaining the objective pursued by the controller: and (ii) whether the objective of the controller could not be achieved by less intrusive means. For this purpose, the Commissioner proceeded to assess the email dated the 17th January 2023, wherein the controller requested the complainant to "*provide us Lab Result reports to processes* [sic] *your claim further*".

10. As a preliminary point, the Commissioner noted that the controller processes '*data concerning health*', which article 4(15) of the Regulation defines 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 his or her health status*'. This constitutes a special category of personal data in terms of article 9(1) of the Regulation, which therefore merits heightened protection due to the risks posed by the processing of the data related to health.

11. Whilst article 9(1) of the Regulation prohibits the processing of special categories of personal data, article 9(2) specifies derogations under which special categories of data may be processed.

Legal Basis

12. In accordance with the specification clause under article 9(4) of the Regulation, Member States are permitted to introduce additional conditions which enable the processing of '*data concerning health*'.

13. The national legislator introduced regulations, namely the Processing of Data concerning Health for Insurance Purposes Regulations, Subsidiary Legislation 586.10 (the **"Subsidiary Legislation 586.10"**), which set forth a lawful basis for the companies involved in the '*business of insurance*' and '*insurance distribution activities*' to process '*data concerning health*'. In this regard, regulation 4(1) of Subsidiary Legislation 586.10 states that '*the processing of data*

concerning health shall be deemed ***to be in the substantial public interest*** *when such processing is necessary for the purpose of the business of insurance or insurance distribution activities*' [emphasis has been added]. This is in line with article 9(2)(g) of the Regulation, which provides that the '*processing is necessary for* ***reasons of substantial public interest****, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*'. Thus, Subsidiary Legislation 586.10 provides that the '*business of insurance*' and the '*insurance distribution activities*' constitute a '*substantial public interest*', and within this context, the applicable legal ground for processing a special category of personal data is article 9(2)(g) of the Regulation coupled with one of the lawful bases as set out in article 6(1) of the Regulation.

14. Furthermore, regulation 4(2) of Subsidiary Legislation 586.10 provides that "*the processing referred to in this regulation shall be subject* ***to the suitable and specific measures designed to safeguard the fundamental rights and freedoms of data subjects***" [emphasis has been added]. This requires the controller to implement "*suitable and specific measures*" in order to protect the fundamental rights and freedoms of the data subjects, which fully respect and comply with the principles set out in article 5(1) of the Regulation.

The Principle of Data Minimisation

15. The controller should seek to implement those measures which minimise the interference with the fundamental right of the right to the protection of personal data resulting from the production of documentation. Article 5(1)(c) of the Regulation states that personal data processed by the controller shall be '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'. Recital 39 of the Regulation further adds that '[p]*ersonal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*'.

16. The Court of Justice of the European Union (the "**CJEU**") emphasises that the principle of necessity is the crux of the Regulation. In its case-law, the CJEU held that when the processing of personal data is not based on consent, the controller should ensure compliance with the requirement of necessity, which also results from the '*data minimisation*' principle as set forth in article 5(1)(c) of the Regulation:

*"First, as is apparent from such Article 6, where the data subject has not given consent to the processing of his or her personal data for one or more specific purposes, in accordance with Article 6(1)(a) of Regulation 2016/679, the processing must, as is apparent from Article 6(1)(b) to (f), **satisfy a requirement of necessity.***

*Second, **such a requirement of necessity follows also from the principle of 'data minimisation'**, laid down in Article 5(1)(c) of that regulation, under which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*[4] [emphasis has been added].

17. Furthermore, the CJEU repeatedly held that the principle of data minimisation gives expression to the principle of proportionality[5], and thus, the controller is required to have regard to the rights and freedoms of the data subjects concerned and balance them according to the circumstances of each case whilst also considering the requirements of the controller.

18. The European Data Protection Board (the "**EDPB**") sheds further light on the principle of data minimisation and how it should be applied by controllers in practice. Accordingly, the Guidelines 4/2019[6] provide that "[c]*ontrollers should first of all determine **whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all.** Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle*" [emphasis has been added].

19. It therefore follows that pursuant to the principle of accountability set out in article 5(2) of the Regulation, the controller should be able to effectively demonstrate the necessity to process the personal data for its own purposes. The EPDB in its Guidelines 01/2022[7] states that "[i]*f the controller imposes measures ... which are burdensome, **it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation...***" [emphasis has been added].

---

[4] Case C-77/21, Digi Távközlési és Szolgáltató Kft. vs Nemzeti Adatvédelmi és Információszabadság Hatóság, judgment of the Court (First Chamber) of 20th October 2022, para. 57 and 58.
[5] Case C-268/21, Norra Stockholm Bygg AB v Per Nycander AB, judgment of the Court (Third Chamber) of 2nd March 2023, para. 54.
[6] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on the 20th October 2020, para. 74.
[7] Guidelines 01/2022 on data subject rights – Right of Access, Version 1.0, adopted on the 18th January 2022, para. 70.

The Request for the Test Results

20. In the present case, the complainant argued that the request for a copy of the medical test result is excessive and therefore infringes the provisions of the Regulation. On the other hand, the controller contended that the reason listed in the Claim Form, '*pelvic pain*' was not sufficient to enable the controller to determine the underlying cause due to the fact that '*pelvic pain*' may lead to various underlying causes.

21. The Commissioner examined the correspondence exchanged between the parties after the controller requested the complainant to produce copies of the test results. By means of an email dated the 17th January 2023, the controller informed the complainant that "[a]*ccording to the terms and conditions we need copy of result reports to processes [sic] your claim*" and cited clause 6.1 of the Health Insurance Policy. Clause 6.1 is being reproduced hereunder:

> 6.1 Out-patient treatment
>
> **Always visit your general practitioner for each new medical condition. The GP will complete part 5A of your claim form.**
>
> **If you need further treatment, the specialist will complete part 5B of the claim form. All specialist consultations must be GP-referred. We will only make an exception for consultations with a gynaecologist or paediatrician for children up to 10 years of age.**
>
> **Send us the completed claim form within two months of the date of your first treatment, with original receipts for consultations and any tests. We will also need a copy of your test results.**
>
> **If your medical condition persists for over three (3) months you may be required to obtain another GP referral prior to seeking specialist advice for the same medical condition.**

22. Furthermore, this requirement is also reflected in the Health Insurance Claim Form, which states that the "*claim form, original receipts, **copies of test results** and other relevant documentation **must be sent to us** ...*" as shown hereunder:

23. The Health Insurance Policy and the Health Insurance Claim Form contradict the information submitted to the Commissioner during the course of the investigation, wherein the controller stated that it does not generally request copies of the test results to process health claims. The Commissioner requested the controller to clarify this conflicting information. The controller explained that:

> "[redacted] ***do have specifically written in their T&Cs that a copy of any tests done should be submitted to*** [redacted] ***as was evidenced in the attachment.*** *It is a market practice that whenever an insurer is unclear about a claim, more information/clarification is required.* ***A fact which is not clearly specified in our T & Cs and it is our intention to match the T & Cs with our current procedures.*** *This is the first time we had someone totally adamant not to provide copies of the test done.* ***We were not aware of the discrepancy previously and this will be rectified in the near future to avoid similar repeats.***" [emphasis has been added].

24. The Commissioner emphasises that the processing of the test results in a general and indiscriminate manner runs contrary to the principle of data minimisation. The controller submitted that '*the Company* ***does not normally*** *request additional evidence when processing a health claim*'. However, this does not result from the Health Insurance Policy and the Health Insurance Claim Form. The policy contractually binds the holder of the insurance cover with the terms and conditions contained therein. The text of such policy is unequivocal and leaves no room for interpretation - **claimants are required to provide copies of the test results when submitting their claim**. It is therefore abundantly clear that the request for a copy of the test result is not a request for "*additional evidence*", but is a requirement imposed by the controller on policy holders.

25. The Commissioner is of the considered view that the test results should only be required in very specific circumstances, and where the intended objective of the controller could not reasonably be achieved by other means less restrictive of the fundamental rights and freedoms of data

subjects. This assessment necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of each case, and in the context of which, account must be taken of the significance of the right to the protection of personal data.

26. In such case, the controller argued that a copy of the test result was necessary because the '*consultant's report indicated the reason to be 'pelvic pain' on the claim form. The underlying medical cause was not clearly identified from the information provided on the claim form*'. The controller further explained that '*pelvic pain*' which is the information listed in the field '[d]*etails of the symptoms/medical condition*' of the Claim Form, could be the result of a variety of medical conditions, some of which would not be covered by the Policy. This shows that solely providing the symptoms is not sufficient and the controller also necessitates the medical cause to be able to process the claim.

27. For this reason, the Commissioner proceeded to assess the Health Insurance Claim Form, in particular, Section 5 which requires the general practitioner and the specialist to provide information in relation to the assessment of the patient's medical condition. The Commissioner noted that the field '[d]*etails of the symptoms/medical condition*' does not request the medical professionals to indicate the medical cause or state the diagnosis. This could in in fact lead to ambiguity as rightly pointed out by the complainant.

28. In this respect, the controller may seek to determine which information is necessary to be provided by the medical professionals in order to limit the requests for the test results and process the data in the least intrusive manner, whilst also ensuring that the controller's business requirements are met. In the event that the controller considers that the Claim Form should be amended to request additional information from the general practitioner and, or the specialist about the claimant's medical situation, such as the medical cause, the Commissioner strongly encourages the controller to undertake a thorough and careful assessment designed to ascertain that the specific request indeed complies with the principles relating to processing of personal data set out under article 5 of the Regulation.

29. This is naturally without prejudice to the fact that in the present case, the controller did not manage to submit evidence to prove that the request for a copy of the test results was indeed adequate and relevant for the purpose of verifying the eligibility of the claim and that this objective could not be achieved by less intrusive means or methods. From the correspondence exchanged between the parties, the Commissioner could note that the controller did not request the complainant to submit any additional information or clarifications, but immediately

proceeded to request him to "*provide us Lab Result reports to processes* [sic] *your claim further*" in accordance with section 6.1 of the Health Insurance Policy.

On the basis of the foregoing considerations, the Commissioner is hereby concluding that the controller failed to effectively demonstrate that the request for a copy of the test results was indeed adequate, relevant, and limited to what is necessary in relation to the purpose sought to be achieved. Furthermore, section 6.1 of the Health Insurance Policy and the Health Insurance Claim Form are requesting the claimants to provide a copy of the test results in a general and indiscriminate manner. These elements do not reflect the principle of data minimisation and leads the Commissioner to decide that the controller infringed article 5(1)(c) of the Regulation.

In terms of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to revise the Health Insurance Policy and the Health Insurance Claim Form in such a manner to comply with the principle of data minimisation.

The controller shall implement the order within twenty (20) days from the date of receipt of this decision and inform the Commissioner of the action taken immediately thereafter.

Non-compliance with this order shall lead to an administrative fine in terms of article 83(6) of the Regulation.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2023.08.10 14:32:51 +02'00'

Ian Deguara
Information and Data Protection Commissioner

Right of Appeal

The parties are hereby being informed that 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 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.

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'.