idpc

Information and Data Protection Commissioner

CDP/COMP/362/2022

[redacted]

vs

[redacted]

THE COMPLAINT

1. On the 5th of September 2022, [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**") against [redacted] (the "**controller**" or '[redacted]'). In her complaint, [redacted] contented that the controller has committed a serious infringement to her data protection rights.

FACTS OF THE CASE

2. For the purpose of this complaint, the Commissioner assessed the relevant facts surrounding the case, whereby she alleged that:

    i. on the 10th of June 2022, she discovered that the contact details, namely the mobile phone number and email address, in the medical files of her children, who share the same father, and whose surname is [redacted], were not hers, but instead those of Ms Jane Doe[2], the partner of the children's father, Mr Joe Doe[3]. The complainant argued that she never authorised this change, which was therefore executed without her consent;

    ii. she discovered this issue when attending to an appointment at [redacted] with her child, which appointment had been cancelled but she was never informed;

[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] Fictious name given by the Commissioner.
[3] Fictious name given by the Commissioner.

iii. her estranged husband and his partner panicked and wanted the complainant to sign documents to sort out the situation, which the complainant refused to do, given that in her views, a data protection breach had occurred as someone had changed her details without her written consent;

iv. when she checked again the children's details, these seemed to have been erased from the system, so that if one entered the children's identity card numbers, no email and mobile number were listed anymore in the system; and

v. that even the complainant's medical file was altered, as her email address and mobile number were removed and replaced with Ms Doe's details. According to the complainant, as a result, Ms Doe got to know all her and her children's medical issues, and all correspondence regarding the complainant's medical appointments, without even being one of their medical consultants. The complainant attached a copy of a ticket of referral showing the contact details of Ms Doe (hereby annexed and marked as '**Doc IDPC1**').

INVESTIGATION

3. The complainant initially sent her complaint by email to the controller and to the Commissioner. Subsequently, on the 6th of September 2022, [redacted] re-submitted her complaint through the dedicated online form available on the Commissioner's website.

Submissions received from the controller

4. On the 6th of September 2022, the controller provided the Commissioner with an update on the internal investigation of the case. The controller outlined the sequence of events in relation to the replacement of the complainant's children contact details on the [redacted]

5. Furthermore, the controller had informed the Commissioner that a meeting had been set with Ms Doe. Consequently, on the 14th of October 2022, the Commissioner requested an update. The controller replied that during the meeting it was explained that when an individual requests a PIN

to access one's [redacted] the details of such person are automatically inputted. The controller added that the [redacted] website[4] clearly stated that, once data is inputted in the [redacted], the [redacted] would be updated with such information, and that any future contact will be based on the information provided.

Ban imposed by the Commissioner

6. On the 17th of November 2022, pursuant to article 58(2)(f) of the Regulation, the Commissioner imposed a ban on the controller and ordered it to take down the [redacted] portal. The Commissioner explained that the [redacted] portal was posing a serious threat to the integrity and confidentiality of [redacted] patients' personal data, as health data was at risk of being disclosed to unauthorised third parties. The portal was designed in manner than anyone in possession of an individual's ID card number and date of birth could effectively replace such individual's contact details with other data, thus effectively being capable of diverting communications addressed to patients, which may contain health data, to third parties. The controller complied with the Commissioner's order and disabled the [redacted] portal.

Request for further information

7. On the 21st of December 2022, the Commissioner requested the controller to provide an update on the action taken on this complaint.

8. By means of a communication dated the 3rd of January 2023, the controller submitted:

   i. that it had requested an audit log of the data processing activities related to the specific complaint, and submitted such reports to Customer Care;

   ii. that the complainant provided an indication of who may have allegedly obtained unauthorised access to the information – upon review of reports, no unauthorised access has materialised as the individual who was identified did not have access to any of the respective [redacted] System; and

[4] *Ibid.*

iii. that from the reports under audit, there was no indication that unauthorised data processing on the IT systems was made. The controller held that it is still reviewing all access times as verification of each role needs to be identified and it is too generic in nature.

9. On the 17th of February 2023, the Commissioner requested the controller to submit:

   i. a copy of the logs related to the changes in the contact details of the complainant and of her two children for the period running from the 21st of November 2021 to the 30th of November 2022; and

   ii. a copy of the notifications, sent both by email and SMS, relating to medical appointments of the complainant and her two children, for the period from the 21st of November 2021 to the 30th of November 2022. The Commissioner specified that these should show the content of the notifications.

10. On the 9th of March 2023, the controller provided the Commissioner with the requested logs. Regarding the copies of the notifications, the controller submitted a list of appointment information relating to the complainant and her children, as logged on [redacted] and held that:

   i. from the system logs, no SMS appointment notification was sent during the mentioned period of time; and

   ii. email notifications are not automated or scheduled but are [redacted] user dependent and may be triggered when an appointment letter is printed to the registered email address. The Controller provided the Commissioner with a sample email notification (hereby annexed and marked as '**DOC IDPC2**').

11. On the 22nd of March 2023, the Commissioner requested the controller to provide the date for each appointment notification relating to the complainant and her children, and the email address to which the notification was sent.

12. On the 24th of March 2023, the controller replied that email notifications are only triggered when a system user attempts to print an appointment letter, and that logs were reviewed for all listed appointments to identify print jobs. The controller stated that there was one case where an employee printed the letter which triggered the print job email, namely an appointment of the complainant scheduled for the 26th of September 2021, which was booked on the 1st of September

2021 and registered as attended. The controller maintained that the email should have been triggered from the system, but no confirmation could be provided by the controller as to whether such email was delivered or received by the third-party solution. The controller outlined that, at the time, the email on its systems was that of Ms Doe.

Extended Commissioner's investigation with MITA

13. On the 5th of April 2023, pursuant to article 58(1)(a) of the Regulation, the Commissioner requested [redacted] to provide the logs of the outgoing email server of the no-reply mailbox used by the controller to send out appointment notifications from the 21st of November 2021 to the 30th of November 2021 concerning any email sent to the email addresses of the complainant and that of Ms Doe.

14. [redacted] replied to the Commissioner's request and informed him that the information requested was no longer available as, in terms of their internal data backup retention timeframes policy, tracking logs are kept for ninety (90) days. Consequently, the indicated dates fell outside the scope of such period.

LEGAL ANALYSIS AND DECISION

15. In essence, the complainant contented that, her contact details on the controller's system were replaced, without her authorisation, with those of Ms Doe and, as a result, the latter obtained unauthorised access to her, and her children's medical records.

16. Article 25(1) of the Regulation provides that the controller shall implement appropriate technical and organisational measures which are designed to implement the data protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements and protect the rights and freedoms of data subjects. The European Data Protection Board Guidelines on Article 25 Data Protection by Design and by Default[6] (the "**Guidelines**") provide that both appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing.

[5] [redacted]

[6] European Data Protection Board, *Guidelines 04/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, Adopted on 20 October 2020.

17. The data protection principles are listed under article 5 of the Regulation, and the principle of integrity and confidentiality, as held in article 5(1)(f) of the Regulation, stipulates that "*personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against* ***unauthorised or unlawful processing*** *and against accidental loss, destruction or damage, using appropriate technical or organisational measures*" [emphasis added].

18. The European Union Agency for Cybersecurity (ENISA) defined the confidentiality requirement as the "*property that information is not made available or disclosed to unauthorized individuals, entities, or processes*[7], and explained that "[i]*n practice, all the measures implemented to ensure confidentiality are designed to prevent the information from being accessed by unauthorized individuals, entities or processes, while ensuring that the authorized individuals, entities processes have access to it*"[8].

19. The ENISA also advised that a "*[l]oss of confidentiality occurs when the information is accessed by parties who are not authorized or don't have a legitimate purpose to access it*"[9]. Similarly, according to the European Data Protection Supervisor, the "*unauthorised or accidental disclosure of, or access to, personal data which is about getting knowledge of personal data by an entity not entitled to this knowledge*" [10] is a form of confidentiality breach.

20. Recital 78 of the Regulation provides that one of the data protection by design and by default ("the **DPbDD")** measures could consist of enabling the controller to "*create and improve security features*". Along with other DPbDD measures, Recital 78 suggests a responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Hence the controller is duty bound to protect the integrity and confidentiality of personal data undergoing processing, and to refrain from any action which may compromise it, such as unauthorised disclosure.

21. The Guidelines provide that key design and default integrity, and confidentiality elements may include risks analysis, whereby the controller shall assess the risks against the security of personal data by considering the impact on individuals' rights and counter identified risks.

---

[7] ENISA, *Guidelines for SMEs on the security of personal data processing*, December 2016, page 10.
[8] *Ibid.*
[9] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, Working Document, v1.0, December 2013, page 5.
[10] EDPS, *Guidelines on personal data breach notification For the European Union Institutions and Bodies*, 2018, para. 27.

22. During the investigation, the Commissioner established that the [redacted] portal posed a risk to the rights and freedoms of the data subjects. For this reason, it imposed a ban on the processing activity carried out therein by the controller, which ban was upheld by the controller[11].

23. The Commissioner established that when an individual requests a PIN to either access one's [redacted] or to [redacted], the inputted details of such person were automatically replacing the previous data.

24. The controller declared that in this case "*there was one case where an individual printed the letter which triggers the above-mentioned print job e-mail*[12]", and that "*at the time the email was xxxx@hotmail.com*[13]". Hence, the complainant's email containing health data was sent to a third party, since the system was designed in a manner that if a third party is in possession of an individual's ID card number and date of birth, they could effectively replace such individual's contact details with other data.

25. By means of this design flaw, one was unintentionally capable of diverting communications addressed to the rightful patients to third parties with the consequence of disclosing personal data in an unauthorised manner.

Based on the foregoing considerations, the Commissioner hereby decides that the controller failed to prevent an unauthorised disclosure by adopting the appropriate technical and organisational measures when implementing the [redacted] portal. This constitutes an infringement of article 5(1)(f) and 25 of the Regulation and, in terms of article 58(2)(b) of the Regulation, the Commissioner is hereby serving the controller with a reprimand.

Furthermore, the ban imposed by the Commissioner on the 17th of November 2022 ordering the controller to take down the [redacted] portal, shall remain in force.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2023.06.26 14:57:49 +02'00'

Ian Deguara
Information and Data Protection Commissioner

[11] *Supra*, § 6.
[12] The controller explained that emails are triggered when a system user attempts to print an appointment letter.
[13] The third party's email address.