idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

Information and Data Protection Commissioner

CDP/COMP/145/2024

[redacted]

vs

[redacted]

COMPLAINT

1. On the 9th April 202[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"** or **"GDPR"**), alleging that [redacted](the **"controller"**) failed to fully comply with his request to access his personal data by omitting his transaction history.

2. As supporting documentation, the complainant provided a copy of the subject access request dated the 31st January 2024, as well as a copy of the reply provided by the controller. In this reply, the controller informed the complainant that "*transaction and gaming data in the transaction history and in the gaming history are no personal data within the meaning of the GDPR*". Moreover, the controller held that the complainant is misusing his rights, thereby constituting grounds for refusal under article 12(5) of the Regulation, as the request is deemed excessive. Furthermore, the controller restricted the right of the complainant by invoking a restriction in terms of article 23 of the Regulation and regulation 4(e) of the Restriction of the Data Protection (Obligations and Rights) Regulations, Subsidiary Legislation 586.09 (the "**Subsidiary Legislation 586.09**"). The controller asserted that its refusal to provide the complainant with the requested information serves as a defence against an impending action for payment from the complainant, as his "*sole intention with the assertion of the information requested is to obtain simplified proof of your transactions*".

[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.

[redacted]

2024).

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

INVESTIGATION

3. On the 30th April 2024, pursuant to the internal investigative procedure of this Office, the Commissioner presented the controller with two (2) options: either to provide the complainant with the requested transaction data, or if opting not to do so, to submit all relevant and necessary information demonstrating that the invoked restriction was both necessary and proportionate. Specifically, the Commissioner requested the controller to clarify whether there was an ongoing legal claim and any legal proceedings and to provide the corresponding supporting evidence.

4. In its reply dated 20th May 2024, the controller, through its legal counsel, submitted the following principal arguments for the Commissioner to consider in the legal analysis of the case:

   i. that German law firms have been encouraging people who have used the services of online gaming companies operating in Germany to initiate proceedings against online gaming companies;

   ii. that the controller has received thirty-nine (39) lawsuits from German players, with transaction data requested by these players serving as the basis of their claims and being used as self-admission by the controller in said proceedings;

   iii. that the complainant can obtain the requested data from other institutions, from which, he transferred and received funds to and from the controller;

   iv. that the restriction is being applied in view of the specific circumstances of this case and will be lifted or eased as soon as the current environment evolves;

   v. that releasing more data would prejudice the controller, as the requested data is clearly intended to serve as a sort of discovery procedure and is being used abusively to facilitate the said claims; and

   vi. that the strict way adopted by the controller in implementing this restriction undoubtably meets the necessity and proportionality test.

LEGAL ANALYSIS AND DECISION

5. During the course of the investigation, the Commissioner established that the complainant had exercised his right to access his personal data in terms of article 15 of the Regulation, by means of a request dated the 31st January 2024. In its reply, the controller restricted the right of the complainant to access his transaction data as it argued that it does not constitute personal data and in the belief that the request is predominantly aimed to facilitate litigation. In this context, the Commissioner sought to determine whether the transaction data constitutes as personal data and, if so, whether the restriction invoked by the controller under regulation 4(e) of the Subsidiary Legislation 586.09 is applicable to the current case.

Subject Access Request: Article 15 of the Regulation

6. Article 15 of the Regulation grants data subjects far-reaching rights of access in relation to the processing of their personal data. Its predominance is derived from article 8(2) of the Charter of Fundamental Rights of the European Union (the **"Charter"**), which explicitly refers to the right of access, by stating that *"[e]veryone has the right of access to data which has been collected concerning him or her..."*. This corresponds to the objective of the Regulation which is clearly outlined in recital 10 of the Regulation, that is, to ensure a consistent and high level of protection of natural persons within the European Union.

7. It has been repeatedly stated by the Court of Justice of the European Union (the **"CJEU"**) that this right is instrumental to the exercise of the other data subjects' rights as set forth in the Regulation[3], mainly articles 16 to 19, 21, 22 and 82. Notwithstanding this, the exercise of the right of access is an individual's right and is certainly not conditional upon the exercise of other rights[4].

8. Article 15(1) and (3) of the Regulation gives the fundamental right to data subjects to obtain from the controllers: (i) confirmation as to whether or not personal data concerning them are being processed and, if so, to receive information about the processing activity, and (ii) to receive a copy of the personal data being processed.

---

[3] Case C-487/21, *'FF vs Österreichische Datenschutzbehörde'*, decided on the 4th May 2023: "*In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing, conferred, respectively, by Articles 16, 17 and 18 of the GDPR, as well as the data subject's right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR.*" (para. 35).

[4] European Data Protection Board, *'Guidelines 01/2022 on data subject rights - Right of access'* (Version 2.0), adopted on the 28th March 2023 (para. 12).

9. The CJEU's Advocate General Pitruzzella in his Opinion explained that article 15(1) of the Regulation "*gives specific expression to the right of access to personal data and related information, defining the precise subject matter of the right of access and the scope of application*", whereas article 15(3) of the Regulation "*provides more details as to how that right is to be exercised, specifying in particular the form in which the controller must provide the data subject with personal data, that is to say, in the form of a copy and, therefore, a faithful reproduction of the data*"[5].

10. Given that the right of access is an expression of article 8(2) of the Charter, it is formulated in very broad terms and, as a result, the CJEU adopted a wide interpretation of this article, with specific reference to the judgments delivered in 2023[6]. This is naturally due to the fact that the right of access is the basis for guaranteeing the effective protection of the data subjects' right to the protection of their data. To this end, the controller should seek to handle the request in such a manner to give the broadest effect to the right of access.

11. It is evident from the wording of article 15 of the Regulation, that the law does not require the data subject to justify or give any reasons for a request under the Regulation, and any presumptions, suspicious or hypothetical conclusions which the controller may consider or reach as to what the data subject's reasons are or might be, should not affect the handling of that request as otherwise this would render the right of access futile and ineffective.

12. This is further supported by the interpretation provided by the European Data Protection Board (the "**EDPB**") in its Guidelines 01/2022 published in March 2023, which reads as follows: *"[c]ontrollers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting ... and whether they hold personal data relating to that individual... [F]or example,* ***the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller"***[7] [emphasis has been added].

---

[5] Case C-487/21, Opinion of Advocate General Pitruzzella, delivered on the 15th December 2022, (para. 48 and 49).
[6] Case C-487/21, *'FF vs Österreichische Datenschutzbehörde'*, decided on the 4th May 2023, & and Case C-154/21, *'RW v Österreichische Post AG'*, decided on the 12th January 2023.
[7] Ibid 4 (para. 13).

Transaction Data

13. The controller, in its reply to the complainant's subject access request, held that "*the transaction amounts are no personal data within the meaning of the GDPR*", "*no person can be identified from an amount, e.g. EUR 5 or EUR 50*".

14. The Commissioner notes that the controller's argument that "*no person can be identified from an amount, e.g. EUR 5 or EUR 50*" oversimplifies the concept of personal data under the Regulation. While a standalone transaction amount (e.g., €5 or €50) might not directly identify an individual, the Regulation defines personal data broadly. According to article 4(1) of the Regulation, personal data is "*any information relating to an identified or identifiable natural person.*" This means that data does not have to identify an individual on its own to be considered personal data. Hence, if transaction amounts are combined with other data, such as names, account numbers, payment details, or transaction dates, they can easily identify a specific person or allow identification through correlation with other information.

15. In Breyer vs Germany[8], the CJEU ruled that even dynamic IP addresses could constitute personal data if they can be combined with other information to identity an individual. The Breyer case established the principle that data does not need to directly identify an individual to be considered personal, it qualifies if it can reasonably be linked to an identifiable individual through additional information. Thus, applying this logic to transaction data, while a transaction amount on its own, may not identify an individual, it becomes personal data when associated with identifiable details such as an account number, transactions timestamps and locations, credit card information or information about payees involved in the transaction.

16. The CJEU's Advocate General Sánchez-Bordona in his Opinion explained that "*overly strict interpretation would lead, in practice, to the classification as personal data of all kinds of information, no matter how insufficient it is in itself to facilitate the identification of a user. It would never be possible to rule out, with absolute certainty, the possibility that there is no third party in possession of additional data which may be combined with that information and are, therefore, capable of revealing a person's identity*".

17. Additionally, in the Rynes case[9], the CJEU affirmed the broad interpretation of personal data, establishing that information which, when combined with other data, can identify an individual,

[8] C-582/14
[9] Rynes v. Úřad pro ochranu osobních údajů (CJEU, 2014) – Case C-212/13

qualifies as personal data. Therefore, transaction amounts, when linked to other identifying information may constitute part of a dataset that meets the definition of personal data under the Regulation. The controller's argument seems to overlook this relational aspect of personal data recognised by the Regulation, presenting an overly narrow view that conflicts with the CJEU interpretations of the Regulation. The fact that a single data point, such as the transaction amount, does not identify a person in isolation does not preclude it from being considered personal data when aggregated with other identifiers.

18. Moreover, the scope of the right to access includes all "personal data" as defined in article 4(1) of the Regulation and includes all information relating to a data subject, no matter in which system, format or way the personal data is processed. It also covers information that is stored in other means than automated means, if the personal data is stored or intended to be stored in a "filing system" within the meaning of article 4(6) of the Regulation.

19. Furthermore, in accordance with the European Data Protection Board Guidelines 01/2022 on Data Subjects Rights - Right of access[10], personal data shall also include observed data or raw data provided by the data subject by virtue of their use of the service or device, such as transaction history. Thus, transaction history is identified among the types of data controllers are expected to provide.

20. In light of the foregoing, the Commissioner dismisses the controller's argument that transaction data does not qualify as personal data.

Restriction in terms of Subsidiary Legislation 586.09

21. Primarily, the Commissioner notes the inconsistency in the controller's approach. While the controller argued that transaction data does not constitute personal data and therefore would not be subject to the complainant's access request under article 15 of the Regulation, it simultaneously invoked a restriction on the grounds provided by regulation 4(e) of Subsidiary Legislation 586.09. This contradictory stance raises questions as to the validity and coherence of the controller's argument. Specifically, if the controller genuinely believed that transaction data does not qualify as personal data, it would logically follow that no restriction would need to be applied under the Regulation, as restrictions only pertain to personal data.

[10] Version 2.0 adopted on 28th March 2023.

22. This contradiction undermines the controller's position and casts doubt on the basis for invoking the restriction. The Commissioner's comprehensive analysis therefore considers the inconsistency between the controller's claim that transaction data is not personal data and its simultaneous reliance on a restriction applicable solely to personal data.

23. Notwithstanding this inconsistency, the Commissioner will proceed to conduct a thorough analysis of whether the restriction invoked by the controller under regulation 4(e) of Subsidiary Legislation 586.09 is applicable to the present case.

24. Recital 4 of the Regulation provides that the right to the protection of personal data is not an absolute right, and it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This has been reaffirmed by the CJEU in the judgment of Facebook Ireland and Schrems[11].

25. The fundamental right to the protection of personal data may be subject to some limitations pursuant to article 52(1)[12] of the Charter. This therefore means that the limitations should be provided by law, respect the essence of the rights and freedoms, and be necessary and proportionate to genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. Therefore, a restriction should not be extensive and intrusive in such a manner that it would void a fundamental right of its basic content.

26. Whereas the Regulation does not define the term *'restrictions'*, the EDPB defines it *"as any limitation of scope of the obligations and rights provided for in Articles 12 to 22 and 34 GDPR as well as corresponding provisions of Article 5 in accordance with Article 23 GDPR"*. The EDPB further provides that a *"restriction to an individual right has to safeguard important objectives, for instance, the protection of rights and freedoms of others or important objectives of general public interest of the Union or of a Member State which are listed in Article 23(1) GDPR. Therefore, restrictions of data subjects'* ***rights can only occur when the listed interests are at stake and these restrictions aim at safeguarding such interests***"[13] [emphasis has been added].

---

[11] Case C-311/18, *'Data Protection Commissioner vs Facebook Ireland and Maximillian Schrems'*, decided on the 16th July 2020 (para. 172).

[12] Article 52(1) of the Charter provides that: "*1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*"

[13] European Data Protection Board, *'Guidelines 10/2020 on restrictions under Article 23 GDPR'* (Version 2.0), adopted on the 13th October 2021 (para. 8).

27. The scope of the obligation and right provided for in article 15 of the Regulation may be restricted by national legislation. To this effect, regulation 4(e) of Subsidiary Legislation 586.09 provides that *"[a]ny restriction to the rights of the data subject referred to in Article 23 of the Regulation shall only apply where such restrictions are a necessary measure required: (e)* ***for the establishment, exercise or defence of a legal claim and for legal proceedings which may be instituted under any law****"* [emphasis has been added].

28. Regulation 7 of Subsidiary Legislation 586.09 makes it abundantly clear that any restriction must be a *"necessary and proportionate measure"*, which effectively means that an assessment needs to be undertaken by the controller on a case-by-case basis to determine whether such measure is indeed "*a necessary and proportionate measure*", rather than merely refusing to comply with a request.

29. Pursuant to article 5(2) of the Regulation, the controller must be able to concretely demonstrate how the restriction is indeed necessary and if this part of the test is passed, the controller must proceed to show the element of proportionality. The case law of the CJEU emphasises that any limitation to the rights of the data subjects must pass a strict necessity test. In C-73/07, the CJEU held that *"derogations and limitations in relation to the protection of personal data ... must apply only insofar* ***as is strictly necessary****"*[14][emphasis has been added].

30. Thus, in his assessment, the Commissioner analysed the reply provided by the controller to the complainant, wherein the data subject was not provided with the transaction history pursuant to regulation 4(e) of Subsidiary Legislation 586.09.

31. The context within which the controller invoked the restriction could only be justified if the controller concretely demonstrates that **the restriction is indeed necessary to defend a legal claim and legal proceedings which may be instituted by the complainant under any law**. During the course of the investigation, the controller reiterated that the right of the data subject was being restricted on the basis that the *"sole purpose with his request for information is to simplify the recovery of your alleged gambling losses and the assertion of the claim for a repayment of these alleged gambling losses"* and because it "*is necessary for the defense against a claim*". The Commissioner does not consider this reason to be compliant with the objective of the restriction as set forth in regulation 4(e) of Subsidiary Legislation 586.09. The

[14] Case C-73/07, *'Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy'*, decided on the 16th December 2008, (para. 56).

said regulation provides that the right of the data subject may only be restricted *"for ... defence of a legal claim **and** for legal proceedings"* [emphasis has been added]. Thus, the restriction shall only apply if it is necessary for the controller to defend an actual legal claim and legal proceedings which may subsequently be instituted under any law. Hence, the controller cannot invoke the restriction merely on the assumption that the data subject may, following the provision of the information, institute legal action against the controller. Consequently, the Commissioner concludes that the controller failed to provide evidence during the course of the investigation to effectively demonstrate that the complainant brought a legal claim against it, and therefore, the controller did not manage to prove that the restriction of a fundamental right is indeed necessary pursuant to regulation 4(e) of Subsidiary Legislation 586.09.

32. Without prejudice to the above, it must be emphasised that even in the eventuality that there is an actual legal claim and ensuing legal proceedings, for the restriction to apply, the controller shall demonstrate that the application of the restriction is indeed a necessary and a proportionate measure.

On the basis of the foregoing considerations, the Commissioner is hereby deciding:

i. **that the controller's assertion that transaction data does not constitute personal data under the Regulation is inconsistent with interpretations of article 4(1) of the Regulation, which defines personal data broadly as any information relating to an identifiable individual. The Commissioner concludes that transaction data, when combined with other identifying details, fall within this definition and therefore should not have been excluded from the complainant's access request under Article 15 of the Regulation; and**

ii. **that the controller has failed to demonstrate how restricting the right of the complainant, at the time of receipt of the request, was indeed a necessary measure in terms of regulation 4(e) of Subsidiary Legislation 586.09. This therefore led to an infringement of article 15 of the Regulation.**

In terms of article 58(2)(c) of the Regulation, the controller is hereby being ordered to provide the complainant with a copy of his transaction history pursuant to article 15(3) of the Regulation, at the time of receipt of the request.

The controller shall comply with this order without undue delay and by no later than twenty (20) working days from the date of receipt of this legally binding decision and inform the Commissioner immediately thereafter of the action taken.

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

After considering the nature of the infringement, the controller is hereby being served with a reprimand pursuant to article 58(2)(b) of the Regulation and warned that, in the event of a further similar infringement, the appropriate corrective action shall be taken accordingly.

Ian DEGUARA (Signature)

Digitally signed by Ian DEGUARA (Signature)
Date: 2025.02.18 16:29:31 +01'00'

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, 158, Information and Data Protection Appeals Tribunal, Merchants Street, Valletta'*[15].

[15] More details on the appeals procedure are available on our website at the following hyperlink: https://idpc.org.mt/appeals-tribunal/