

Information and Data Protection Commissioner

CDP/COMP/41/2022

[REDACTED]
vs
[REDACTED]

COMPLAINT

1. On the 2nd of February 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 Regulation¹ (the “**Regulation**”) against [REDACTED] (the “**controller**” or [REDACTED]). [REDACTED] operates in the online gambling industry under a license issued by the Malta Gaming Authority³ (the “**MGA**”).
2. In his complaint, [REDACTED] maintained that he was a customer of [REDACTED] and expressed concerns about the processing of his payment information by the controller. In particular, due to the fact that payment descriptors⁴ of some transactions made in favour of the controller led to [REDACTED] a payment operator based in Nigeria, wherein the complainant alleged that such processing took place in Nigeria.

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], Malta.

[REDACTED] last seen on 18th April 2023.

⁵ In its privacy policy on [REDACTED] last seen on 18th April 2023 [REDACTED] identifies itself as “ [REDACTED]”

3. Prior to filing his complaint with the Commissioner, the data subject had contacted the controller about the matter. The controller replied that it had transferred the data to [REDACTED] payment aggregator, which was responsible for providing [REDACTED] with credit card payment options. The controller also sustained that the payment system which finally processed the transactions in question was [REDACTED], and that the payment descriptors that the complainant had in his statement were [REDACTED] payment descriptors.
4. [REDACTED] also sustained that [REDACTED] was not integrated with the casinos under [REDACTED] licence, neither directly nor via other payment aggregators. [REDACTED] explained that while most of the payment processing operations took place on the payment system's side, [REDACTED] received the result of the transaction. [REDACTED] stressed that it never received funds directly into its bank account, and that the deposit was just reflected on the payment system's account until the clearing took place, which meant, that they were not able to configure the miscoding, and never did so.
5. After being informed by [REDACTED] that it was [REDACTED] which processed his transactions, the complainant approached [REDACTED] for clarifications. [REDACTED] replied that it was not the payment gateway that processed those funds, and it guided the complainant to refer the case to [REDACTED].

INVESTIGATION

6. Prior to initiating with the investigation, the Commissioner requested the complainant to list the casinos operated by the controller he was registered with. He replied that "*the casino brands in question were [REDACTED] but few transactions were processed on behalf of this brand*" ([REDACTED] are hereinafter collectively being referred as the "**brands**").
7. The Commissioner also requested the complainant to provide evidence demonstrating that the three transactions having the description starting "[REDACTED] were indeed a result of transactions effected through his activity within his player account held with the controller. The Commissioner further requested the complainant to share all exchanges with [REDACTED] on the subject-matter of his complaint. On the 7th of March 2022, the complainant submitted the requested correspondence.

⁶ [REDACTED] last seen on 18th April 2023.

⁷ [REDACTED] a company registered in Malta with number [REDACTED] and address at [REDACTED] Malta.

8. The complainant held that the only way for him to be able to demonstrate beyond reasonable doubt what was being requested by the Commissioner, was to conduct a reconciliation between the transaction records provided by the controller and his independent bank statements. Accordingly, on the 10th of March 2022, the complainant submitted:

- i. a copy of an email dated 27th of January 2022 sent to the complainant by the controller, whereby the controller provided him with his transaction records. The complainant also submitted a screenshot of these transaction records showing the successful transactions conducted on the 4th of December 2021, being the date of the transactions allegedly processed by [REDACTED] and
- ii. a redacted current bank account and credit card statement, wherein the complainant highlighted certain transactions tallied with those on the document obtained from the controller.

9. On the 24th of March 2022, pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions, including any other information which it deemed relevant to submit in connection with the allegation raised by the complainant for the Commissioner to consider in the legal analysis of the case. More specifically, the Commissioner requested the controller to identify the legal basis for transferring the complainant's personal data to Nigeria.

10. On the 20th of April 2022, the controller replied to the Commissioner's request:

- i. that since its inception date, it never contracted and, or dealt with on a commercial level with [REDACTED] and that therefore, it did not have any relationship with such company;
- ii. that the data flow pertaining to the complainant revolved around a flow from the controller to [REDACTED] for the purpose of payment processing, and on a further data flow to [REDACTED], a payment system contracted by the controller that returned the result of the transactions;
- iii. that the controller contracted directly with [REDACTED] which entities were for all intents and purposes to be considered as joint controllers with [REDACTED] in terms of the data flow in question and within the ambit of article 26 of the Regulation;
- iv. that it was safe to conclude that the data in question was transferred to [REDACTED] in its capacity as payment provider solution, and that therefore any form of data transfer to any country outside the EU / EEA came into effect through [REDACTED] rather than through the controller, as insinuated by the complainant; and

- v. that both [REDACTED] were European entities, and that their engagement as B2C licensees had effectively been approved by the Malta Gaming Authority. From the controller's standpoint, it was inconceivable to attribute any form of fault to the controller with respect to data which was effectively transferred outside of the EU / EEA by [REDACTED] and this since the transfer was beyond [REDACTED] control. The controller stressed that, in its views, it had adhered to all its contractual obligations with both [REDACTED], as well as with its regulatory obligations under the Maltese gaming and data protection framework as the controller.

11. Subsequently, the Commissioner provided the complainant with the opportunity to rebut the arguments made by the controller. Accordingly, by means of an email dated 4th May 2022, the complainant submitted:

- i. that it was pleasing to have established the involvement of the Nigerian-based entity [REDACTED] as an actor in the value-chain of online gaming services provided to the complainant, particularly in light of the previous misrepresentations of [REDACTED] as to the involvement of Flutterwave in [REDACTED] provision of online gaming services and transfer of personal information outside of the EU;
- ii. that [REDACTED] assertion that [REDACTED] was the entity which transferred personal information outside of the EU was previously contented by [REDACTED];
- iii. that he questioned [REDACTED] position that it had no commercial relationship with [REDACTED]. In this respect, the complainant pointed out that [REDACTED] was promoted as a payment partner of [REDACTED] sister casino, [REDACTED]. The complainant suggested that this was an attempt to further mislead the Commissioner, and should be taken into account when assessing the credibility of the statements made by [REDACTED];
- iv. that, in spite of not being in a position to comment on the commercial and contractual relationship between [REDACTED] acting as joint controllers pursuant to article 26 of the Regulation, any assertion by [REDACTED] that [REDACTED] was solely liable was of irrelevance to the complainant who, for all intents, only had a relationship with [REDACTED], and saw his data illegally transferred to Nigeria as a result of such relationship;
- v. that pursuant to article 26(3) of the Regulation, a data subject may exercise their rights in respect of and against each joint controller. The complainant maintained that [REDACTED] never disclosed to him

⁸ *Supra*, § 5.

⁹ The complainant provided the following link: [https://\[REDACTED\]](https://[REDACTED]) last seen on 18th April 2023.

that personal information would have or may have been transferred to Nigeria, a jurisdiction considered as having inadequate data protection safeguards. In this respect, the complainant sustained that in its submissions, the controller made multiple attempts to mislead about the involvement of [REDACTED]. The complainant also added that, as direct contracting party, [REDACTED] should have been held responsible vis-à-vis the breach, and that [REDACTED] should have relied upon appropriate contractual remedies and indemnification in their own relationship with the joint controllers, as this was also a requirement under the Regulation; and

- vi. that he strongly refuted [REDACTED] assertion that the MGA had ultimately ratified [REDACTED] value-chain. In this respect, the complaint held that whilst the MGA was the primary regulatory body for online gaming activities, it was under the jurisdiction of the Commissioner and not of the MGA to determine compliance with the Regulation. The complainant pointed out that the MGA had prepared a paper in consultation with the Commissioner who, in turn, provided guidelines to online gaming operators on compliance with the Regulation. The complainant emphasised that, pursuant to such consultation paper, an undisclosed transfer of personal information to a jurisdiction not subject to an Adequacy Decision by the European Commission did not appear to be contemplated as a lawful act under the Regulation.

12. Pursuant to the Commissioner's complaint-handling procedure, the controller was subsequently provided with the opportunity to rebut the complainant's submissions. On the 13th of May 2022, the controller submitted:

- i. that it refuted the complainant's assertion that [REDACTED] was an actor in [REDACTED] value chain by reiterating that it had never contracted, directly or indirectly, with [REDACTED] for the services rendered under its license with the MGA. In this respect, the controller reiterated that it had a list of approved entities providing it with payment services, given that it was an obligation for such entities to be approved, and that [REDACTED] did not feature in such list. [REDACTED] therefore contended that it has never engaged [REDACTED] as a payment service provider;
- ii. that the link provided by the complainant¹⁰ did not relate to [REDACTED] but rather to [REDACTED] [REDACTED] Ltd ("[REDACTED]"), an entity incorporated under the laws of Nigeria, which had successfully obtained a licence to operate as a gaming operator. The controller explained that in this process, [REDACTED] was obliged to engage a Nigerian payment service provider for payments undertaken under the Nigerian licence, and therefore engaged [REDACTED]. The controller held

¹⁰ *Supra*, footnote 5.

that, in its views, this did not in any way indicate that [REDACTED] was a payment service provider of [REDACTED] under its Maltese licence;

- iii. that [REDACTED] had various companies set up within its group, some of which in Malta and others outside of Malta, with the aim of applying for licences in different jurisdictions. The controller explained that every licence had individual regulatory requirements which needed to be adhered to, but which in no form or manner interlinked the operation of one entity to the other. According to the controller, the only relationship between [REDACTED] and [REDACTED] was that they had common shareholding. The controller therefore concluded that the complainant's argument that the use of [REDACTED] by [REDACTED] associated the services provided by [REDACTED] to [REDACTED] was inapplicable to the matter at hand; and
- iv. that within the relationship between [REDACTED] and [REDACTED], it was [REDACTED] which determined the means of the processing and in doing so, processed cardholder data subject to PCI & DSS to ensure compliance with payment card industry data security standards. According to [REDACTED] in its capacity as merchant service provider, [REDACTED] had full control to determine the final status of the transactions of the company. It was therefore evident, in the controller's views, that [REDACTED] was directly liable for contracting with [REDACTED] without considering the pertinent obligations under the Regulation.

13. On the 23rd of May 2022, the Commissioner requested the controller to provide a copy of the merchant service agreement between [REDACTED] and [REDACTED] ("the Agreement")¹¹ after redacting any commercial and confidential information included therein. On the 25th of May 2022, the controller submitted the requested document.

14. On the 16th of June 2022, considering the controller's position that it was a joint controller with [REDACTED] and [REDACTED], the Commissioner requested a copy of the arrangement entered with those entities pursuant to article 26 of the Regulation. Furthermore, the Commissioner requested the controller to provide evidence to substantiate its statement that "*it is safe to conclude that the data in question was transferred to [REDACTED] by [REDACTED]*"¹².

15. On the 22nd of June 2022, the controller replied by asserting that, insofar as joint controllership with [REDACTED] was concerned, the arrangement pursuant to article 26 of the Regulation was included in the Agreement with [REDACTED] which the controller previously submitted. As of joint controllership with

¹¹ Standard Merchant Acquiring Terms between [REDACTED] and [REDACTED] signed in August 2019.

¹² *Supra*, § 8 (iv).

██████████, the controller held that the required arrangement was included in its agreement with ██████████ and provided an extract. The controller specified that such instrument catered for the provision of “Payment IQ” as a payment gateway pursuant to section 4 thereof.

16. In the same communication, the controller maintained that *“At this stage we are not in a position to provide the evidence to substantiate our statement that “it is further safe to conclude that the data in question was transferred to ██████████”, given that ██████████ unilaterally transferred the data in question to ██████████ and this without notifying our entity as a joint controller under the GDPR. Moreover, we are therefore not in possession of any documents to substantiate this statement, barring the bank statements exhibited by the data subject which clearly show the presence of ██████████ within the payment processing flow”*.

17. On the 8th of July 2022, a meeting was held between the Commissioner and ██████████ to discuss the matter at hand and particularly, the dynamics of the payment transaction flow and its role under data protection law.

18. On the 21st of July 2022, the controller followed up the meeting by submitting a document describing the roles of the actors involved in the payment transactions flow. Therein, the controller explained the role of payment service providers (“PSPs”) in accepting various types of online payments. ██████████ sustained that in the case at hand, ██████████ was a ██████████ and ██████████ a technical integration facilitator for payments allowing online gaming merchants to process payments with different PSPs.

19. ██████████ sustained that, based on the “European Data Protection Supervisor Flowcharts and Checklists on Data Protection”, it had a controller-processor relationship with ██████████. In this respect, ██████████ identified ██████████ as a controller for its own means and purposes, and as a processor in respect of ██████████

20. The controller also stressed that ██████████ was a PSP and that, based on the information provided to the Commissioner, as well as on the facts pertaining to the situation, it was evidently clear that ██████████ did not seek the controller’s prior written authorisation when subcontracting with ██████████, thus determining its own means and purposes in connecting to acquiring banks, cards and payment networks.

21. The controller also submitted a recording of a payment flow done by using both ██████████ and ██████████. moreover, it made a test payment using a non-EU card to stay close to the scenario encountered by the complainant. The controller stressed that therein ██████████ was visible as a payment system and ██████████ as a provider. The controller also provided a bank statement of the card used to make the payment to identify the different parties of the payment flow.

22. On the 25th of August 2022, the Commissioner requested the controller to submit a video of the back-end system of one of the complainant's transactions dated the 4th of December 2021. The controller provided this on the 31st of August 2022.
23. On the 31st of August 2022, the Commissioner approached [REDACTED], and requested it to provide clarifications about its role in relation to the subject-matter of the complaint.
24. On the 5th of September 2022, [REDACTED] declared that it was not a PSP, but rather a reseller of a gateway which processed payment transactions with third party acquirers, which were in several countries, both within and outside the EEA. [REDACTED] further maintained that it did not process any of [REDACTED] clients' personal data, and that it did not act as a processor or as a sub-processor to any of its processors. [REDACTED] clarified that it was neither receiving nor giving instructions to or from [REDACTED] about payment processing, as it was up to [REDACTED] to instruct the platform about the gateway the transaction should have been channeled to.
25. [REDACTED] also held that its understanding was that the controller made use of a third-party gateway provider instructed by the controller to channel the traffic in the gateway, which in this case went to a third-party acquirer based outside of the EEA, with whom [REDACTED] brokered the agreement.
26. On the 30th of September 2022, the Commissioner requested [REDACTED] to specify the third-party acquirer based outside of the EEA with whom it had brokered the agreement. Given [REDACTED] stance, that it did not process any of [REDACTED] clients' personal data and did not act as a processor or as a sub-processor to any of its processors, conflicted with the contents of the agreement between [REDACTED] and [REDACTED]¹³, whereby it was agreed that [REDACTED] would act as [REDACTED] processor in certain instances, the Commissioner requested [REDACTED] to clarify.
27. On the 7th of October 2022, [REDACTED] replied that when the agreement with [REDACTED] was signed, the clauses were quite generic, given that the way they operated at the time could have led [REDACTED] to act as a processor. [REDACTED] also sustained that, had it commenced to act as a processor on behalf of [REDACTED], it would have added a data processing agreement to the merchant agreement, but this did not occur, hence the addendum was not concluded. [REDACTED] added that at no point in time it acted on instructions given by [REDACTED] or by any of its processors, or on their behalf.
28. In the same reply, [REDACTED] sustained that [REDACTED] used a processor for the transaction concerned, during which a processing channel is used to process the transaction which is integrated into a platform

¹³ *Supra*, § 13.

with whom [REDACTED] had a contract. [REDACTED] further held that the platform was integrated into the processing channel through an API which then, sent the transaction to a gateway on [REDACTED] instructions. [REDACTED] maintained that, as far as it was concerned, this could have been any gateway acting as a controller, which not even [REDACTED] was aware of, given that it had no visibility over the data. It was then that the gateway processed the transaction by means of acquirers, some of whom may have been outside of the EEA. [REDACTED] added that it brokered agreements with different gateways and not with the acquirers, and that not being privy to the processing taking place, it would not know which acquirer was used for this particular transaction, as it did not have any contact with them.

29. On the 19th of October 2022, the Commissioner requested [REDACTED] to elaborate on its statement that “as far as [REDACTED] is concerned this could be any gateway acting as a controller”. The Commissioner also requested, considering [REDACTED] claim that it brokered agreements with different gateways, to identify the gateways with whom [REDACTED] brokered the agreement for [REDACTED]

30. On the 31st of October 2022, [REDACTED] answered that [REDACTED] as the merchant and acting as the controller, was at liberty to channel their traffic to any gateway of its choice, and that [REDACTED] was not receiving nor giving instructions to or from [REDACTED] about payment processing. [REDACTED] explained that it was up to the merchant to instruct the platform about the gateway on which the transactions should have been channeled to, and that [REDACTED] was not being made privy to such instructions. [REDACTED] replied to the second question that, following a meeting with [REDACTED], [REDACTED] was informed that in this case, the platform provider [REDACTED] had used [REDACTED] as the payment gateway provider.

31. On the 27th January 2023, the Commissioner informed [REDACTED] that it had extended the investigation to [REDACTED]. Considering that the complainant’s relationship is with [REDACTED], the Commissioner provided [REDACTED] with the final opportunity to clarify its functional role, specifically regarding the processing of the complainant’s personal data in Nigeria.

32. On the 13th of February 2023, [REDACTED] provided its reply to the Commissioner’s request, wherein it put forward the following arguments:

- i. that [REDACTED] utilised the services of [REDACTED] which functioned as a distributor of various payment systems, including but not limited to, [REDACTED]
- ii. that in certain instances, payment systems may receive personal data from [REDACTED] to verify the identity of the payment initiator and account owner, in an effort to prevent unauthorised payments made through third-party funds;

- iii. that in other situations, the customer may directly provide the data to the payment provider upon initiation of payment, which served as a contractual basis. [REDACTED] held that in these cases, [REDACTED] only received information regarding the status of the payment and the initiator;
- iv. that upon receipt of the payment initiation data the PSP, via its card schemes or networks, reached out to the acquirer for further payment processing. According to [REDACTED], these actions remained outside of the purview and control of online service providers making use of PSPs to receive payments for their goods and services;
- v. that therefore, due to the fact that it did not possess comprehensive information and did not exert control over the payment process and data flow, [REDACTED] could not be deemed as the controller for the processing of payments. [REDACTED] sustained that this may be evidenced by all the arguments brought to the Commissioner's attention earlier on in the investigation;
- vi. that it was worth to mention that PSPs were regulated by Directive (EU) 2015/2366 (Payment Services Directive), which established, *inter alia*, standards for the required quantity of personal data, security measures and retention periods;
- vii. that [REDACTED] relied on the standard merchant acquiring terms with [REDACTED], in particular part 7 thereof, titled "Data Security and Privacy", which provided [REDACTED] with guidance on the security requirements for processing personal data, the possibility of an audit by [REDACTED], and the obligation to promptly notify [REDACTED] in case of a security data breach. The controller pointed out that it was noteworthy that the controller borne the responsibility of informing the relevant supervisory authority in the event of a personal data breach;
- viii. it quoted two examples from a set of guidelines by the European Data Protection Board¹⁵ (the "EDPB") and from a document published by the UK Information Commissioner's Office¹⁶ in support of its position that PSPs operated as independent controller and borne full responsibility for the processing they conducted;

¹⁴ *Supra*, § 13.

¹⁵ EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 1.0, Adopted on 02 September 2020, § 38, second example.

¹⁶ UK ICO, *Contracts and Liabilities between Controllers and Processors*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/>, last seen on 18th April 2023.

- ix. that it was therefore challenging to classify the acquirer and the PSP as processors, given that they held significant influence over the purpose and method of processing, often deciding independently based on local laws and card scheme regulations what data to process, how long to retain the data for correct payment processing, the technical means to use for processing, and with whom to share the data;
- x. that [REDACTED] previous characterisation of the payment provider as a processor was based solely on the language of section 7.7 of the agreement between [REDACTED] and [REDACTED]¹⁷;
- xi. that, regarding [REDACTED] assertion that it was not involved in the data processing, [REDACTED] clarified that during the discussion between [REDACTED] and [REDACTED] about the complaint, [REDACTED] stated that they have used [REDACTED] as a payment gateway. On this aspect, [REDACTED] stressed that it had no connection with such legal entity or payment gateway, and that it did not enter into any legal agreement with [REDACTED] maintained that all disputed payments in its system were marked as processed by [REDACTED] with whom [REDACTED] had directly executed the agreement;
- xii. that its privacy policy acknowledges that its service providers may have, in certain circumstances, transferred users' data outside of the EEA:
- "In order to provide you with an efficient service, we and/or our service providers might require transferring your personal data from one country to another in the European Union (EU) and European Free Trade Association (EFTA) regions and also to some data processors that may be based outside of the European Economic Area (EEA). We shall always use our best efforts to ensure that your information and data is treated securely and in accordance with this Privacy Policy"*.
- xiii. that in this instance, the complainant's allegations regarding the unauthorised transfer of his personal data outside of the EEA during payment processing were unfounded;
- xiv. that upon registration, users were required to acknowledge their familiarity with the terms of service and with the privacy policy through the act of clicking a checkbox;

¹⁷ *Supra*, § 13.

- xv. that payment processing was conducted in accordance with the contractual obligations established between the user of the service and the service itself, as it was the user to initiate the payment transaction; and
- xvi. █████ requested the Commissioner to consider that the complainant initially made a demand for compensation for the entirety of his losses incurred while utilising the services provided by the controller. █████ also held that the complainant threatened to file a complaint with the Commissioner and with other relevant gambling regulatory bodies if the said compensation was not granted.

LEGAL ANALYSIS AND DECISION

33. As a first step in the legal analysis of the case, the Commissioner examined the allegation made by the complainant against █████ namely that █████ processed his personal data in Nigeria by transferring it to █████. The complainant asserted that such processing amounted to an infringement of the Regulation, since Nigeria is a non-adequate third country¹⁹.
34. The Regulation acknowledges that the scale of the collection and sharing of personal data has increased significantly, and that technology should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data²⁰.
35. The Regulation further recognises that flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. In this respect, the Regulation makes it clear that when personal data are transferred from the Union to controllers, processors, or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by the Regulation should not be undermined²¹.
36. Transfers to third countries and international organisations may only be carried out in full compliance with the Regulation. A transfer could take place only if, subject to the other provisions of the Regulation, the conditions laid down in the provisions of the Regulation relating to the transfer

¹⁸ *Supra*, § 2.

¹⁹ *Supra*, § 11(vi).

²⁰ Recital 6 of the Regulation.

²¹ Recital 101 of the Regulation.

of personal data to third countries or international organisations are complied with by the controller or processor²².

37. As held by the EDPB, the Regulation does not provide for a legal definition of the notion “*transfer of personal data to a third country or to an international organisation*” (a “**transfer**”)²³. To that end, the EDPB has identified the following three cumulative criteria to qualify a processing operation as a transfer:

- i. a controller or a processor (the “**exporter**”) is subject to the Regulation for the given processing;
- ii. the exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor (the “**importer**”); and
- iii. the importer is in a third country, irrespective of whether or not the importer is subject to the Regulation for the given processing in accordance with article 3 thereof, or is an international organisation.

38. In the present case, the complainant implicitly identified [REDACTED] as the exporter, and [REDACTED] as the importer. As of the second requirement of the transfer, being that there was disclosure by transmissions or personal data made available by the exporter to the importer, the complainant provided a list of some transaction descriptors²⁴.

39. By definition, “disclosure by transmission” can only occur between a minimum of two, separate parties. It follows that, *conductio sine qua non* that the exporter party discloses personal data by transmission, or makes it available, to the importer by means of a positive action. Based on these considerations, an empirical link between the exporter and the importer, being the positive action of disclosure by transmission, must be present for a transfer to occur.

²² *Ibid.*

²³ EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0, Adopted on 14 February 2023, § 7.

²⁴ *Supra*, 2.

40. Having duly perused the evidence provided by the complainant in his initial complaint and gathered during the course of the investigation²⁵, including the information obtained from both [REDACTED] and [REDACTED], the Commissioner established that these are not sufficient to establish that the above-mentioned positive action took place, and that therefore, a transfer by [REDACTED] to [REDACTED] was affected.

41. The Commissioner proceeded to read article 24 of the Regulation which imposes accountability obligations on the controller, alongside article 5(2) thereof. The principle of accountability is one of the central pillars of the Regulation and one of its most significant innovations. It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance²⁶.

42. Recital 74 of the Regulation provides that the responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In this respect the principle of responsibility, together with other more specific rules on how to comply with the Regulation and about the distribution of responsibility, require the controller to have a clear overview of the personal data undergoing processing and about the roles of the different actors in respect of the processing of such data. Such roles are those of the controller, joint controller and processor.

43. The concepts of controller, joint controller and processor play a crucial role in the application of the Regulation, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice²⁷. In addition to this, pursuant to the Regulation, it is an obligation to conclude legal arrangements between the entities undertaking such roles²⁸, which arrangements constitute organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation which the controller is duty bound to implement²⁹.

²⁵ *Supra*, Investigation part.

²⁶ Docksey, Christopher (2020). Article 24: Responsibility of the controller. In Kuner, Christopher; Bygrave, Lee Andrew & Docksey, Christopher (Ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, page 557.

²⁷ EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 2.1, Adopted on 07 July 2021, page 3.

²⁸ Article 26 of the Regulation mandates that an arrangement is in place between joint controllers, whereas article 28 thereof requires that an agreement is concluded between the controller and the processor.

²⁹ See Article 24(1) of the Regulation.

44. Unless these roles are agreed upon and established, without the necessary legal arrangements in place, compliance with the Regulation cannot be achieved. This is even more required to ensure that the data subject maintains control over his or her personal data.
45. Initially, [REDACTED] alleged that it was safe to conclude that [REDACTED] transferred the complainant's personal data to [REDACTED]³⁰. Following that, the Commissioner requested [REDACTED] to submit evidence to demonstrate this allegation³¹. [REDACTED] replied that it was in not a position to provide such evidence³².
46. As of its relationship with [REDACTED], from a data protection perspective, and the relative roles with reference to the processing activity at stake, [REDACTED] held that it was a joint controller with [REDACTED] pursuant to article 26 of the Regulation³³.
47. Given that it is an obligation for joint controllers to determine, in a transparent manner, their respective responsibilities for compliance with the obligations under the Regulation, as regards the exercising of the rights of the data subject and their respective duties in terms of transparency by means of an arrangement between them, the Commissioner requested [REDACTED] to submit a copy of such arrangement³⁴.
48. [REDACTED] replied that the arrangement was found in its agreement with [REDACTED]. However, by perusing this document, the Commissioner did not find any reference to joint controllership between N1 and [REDACTED], nor any information which could lead to assume that [REDACTED] and [REDACTED] were indeed joint controllers.
49. Subsequently, in contradiction with what stated earlier on, [REDACTED] submitted that in the relationship between [REDACTED] and [REDACTED], it was [REDACTED] which determined the means of the processing and, in doing so, processed cardholder's data pursuant to PCI & DSS in order to ensure compliance with payment card industry data security standards³⁶, thus implying that [REDACTED] was the (only) controller regarding the processing activity in question.

³⁰ *Supra*, § 10 (iv).

³¹ *Supra*, § 14.

³² *Supra*, § 16.

³³ *Supra*, § 10 (iii).

³⁴ *Supra*, § 14.

³⁵ *Supra*, § 15.

³⁶ *Supra*, § 12.

50. Later, again in an inconsistent fashion, █ declared that it had a controller-processor relationship with █, thus identifying █ as a processor in respect of █³⁷.

51. Finally, in its latest submissions, █ declared once again that PSPs were controllers rather than processors³⁸, which meant that █ was a controller in the specific processing activity.

52. It is clear from the preceding paragraphs that, at the time of the determination of the means and purpose for processing, █ did not take steps to establish the relationship between █ and █ in relation to the processing and failed to conclude the necessary legal arrangements. As a matter of fact, and as reported above, █ changed its position on such relationship multiple times during the investigation, which demonstrates serious negligence. This runs contrary to the principle of accountability contemplated in the Regulation and particularly, in article 24(1) thereof.

53. Further to the above, and even more grievously, █ declared that “[i]n certain instances, payment systems may receive personal data from █ Interactive to verify the identity of the payment initiator and account owner [...]. In other situations, the customer may directly provide the data to the payment provider upon initiation of the payment [...]”.

54. This statement indicates that █ does not have full cognisance, and is not able to distinguish in practice, those instances where █ transfers personal data to a payment system, and where the payment system gathers the personal data directly by itself. On the contrary, █ should be fully aware of the dynamics of any such transfer in view of making sure that these abide by the provisions of the Regulation.

55. In its final submissions, █ also pointed out that its privacy policy informs data subjects that its service providers may, in certain circumstances, transfer users’ data outside of the EEA, and that upon registration for its services, users were required to acknowledge their familiarity with the terms of service and privacy policy by clicking a checkbox³⁹.

56. Article 13 of the Regulation requires that data subjects are informed by the controller about the details of the processing at the time when the controller collects the data directly from the data subject. This enshrines a positive obligation on the controller, which requires that the controller

³⁷ *Supra*, § 19.

³⁸ *Ibid*.

³⁹ *Supra*, § 32 (xii).

provides a set of required details about the processing operation, which is usually contained in a data protection policy, which includes, *inter alia*, the identity and contact details of the controller, the purposes of the processing for which the personal data are intended, the legal basis for the processing, the recipients of the personal data, and the right to exercise right of the data subjects.

57. Article 13(1)(f) thereof prescribes that, where applicable, the controller shall provide information about the fact that the controller “*intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available*”.

58. The controller is therefore duty-bound to provide information about the transfer of personal data to a third country or international organisation to the data subject, and such information shall be combined with supplementary information about the transfer, as specified in the provision cited above.

59. In the present case, in its privacy policy, [REDACTED] limited itself to say that it could have transferred personal data to “*some data processors that may be based outside of the European Economic Area (EEA)*”, without providing any of the details required by the second part of article 13(1)(f) of the Regulation.

Based on the foregoing considerations, the Commissioner hereby decides that the controller infringed:

- i. article 24(1) of the Regulation, for failing to implement appropriate organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the Regulation; and**
- ii. article 13(1)(f) of the Regulation, for failing to include in its privacy policy information about the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in article 46 or 47, or the second subparagraph of article 49(1), reference to the appropriate or suitable safeguards.**

In terms of article 58(2)(b) of the Regulation, the Commissioner is hereby issuing a reprimand to the controller.

As a result, pursuant to article 58(2)(d) of the Regulation, the Commissioner is ordering the controller to bring the processing operation into compliance with the provisions of the Regulation, by adopting a data protection policy that contains all the requirements of article 13(1)(g) of the Regulation, and which shall be made available to all the data subjects at the time of collection of their personal data.

The controller shall provide the Commissioner with evidence of compliance within one (1) month from the date of receipt of this legally-binding decision. Non-compliance with the order of the Commissioner within the stipulated timeframe shall be subject to an administrative fine pursuant to article 83(6) of the Regulation.

Ian
DEGUARA
(Signature)

Digitally signed
by Ian DEGUARA
(Signature)
Date: 2023.04.19
12:27:25 +02'00'

**Ian Deguara
Information and Data Protection Commissioner**