Athens, 09-03-2022 Prot. No.: 618 DECISION 11/2022 (Department) The Personal Data Protection Authority convened, at the invitation of its President, in a regular meeting in the composition of the Department at its headquarters on 10/11/2021 and 10:00 a.m., in order to examine the case referred to in the present history. The meeting was attended by teleconference by Georgios Batzalexis, Deputy President of the Authority, Konstantinos Menoudakou, and regular members, Konstantinos Lambrinoudakis and Charalambos Anthopoulos. Alternate member Grigorios Tsolias was also present, as rapporteur with the right to vote. Regular member Spyros Vlachopoulos did not attend due to disability, even though he was legally summoned in writing. The meeting was attended, by order of the President without the right to vote, by Haris Symeonidou, specialist scientist - auditor as assistant rapporteur and Irini Papageorgopoulou, employee of the Administrative Department of the Authority, as secretary. of the President The Authority took into account the following: With no. prot. C/EIS/4720/08-07-2020 her complaint to the Authority, A (hereinafter the complainant), is directed against the OPAP Agency with store code ..., [region X], complaining about illegal processing of her personal data, because on ... an online user account was created on the joker website of OPAP https://joker.opap.gr, with her details, without her knowledge, which was then confirmed at the said Agency using a copy of her police ID. In particular, this complaint states the following: 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 On …, in an attempt to create an online account on the website https: //joker.opap.gr, with username "x" and e-mail address ..., the complainant received a notification from the system that there is already a user account with the same identity information and username "ψ". However, as she herself had not taken a corresponding action in the past, she requested clarifications on the same day, initially from the OPAP user support email address (support@opap.gr), from which she was informed that the account in question was created on ... using e-mail ... . Immediately the complainant replied to the same address: "Please deactivate the account, as it does not belong to me. Please share with me the details that have been declared, as well as the identification documents. All the necessary actions should be taken as this is hacking." Subsequently, the complainant contacted the address of the Data Protection Officer (DPO) of OPAP (dpo@opap.gr), who confirmed that the account in question had been created on ... adding that on the same day it was identified through OPAP agency with store code … (… [region X]). Specifically, on ... the complainant received from the Data Protection Office of OPAP the answer that "for the identification of an online account through an agency, it is necessary to provide documents showing both sides of the candidate player's police ID. In fact, to identify the above account, it seems that a police ID was used, which has the same information as the ones you tried to declare during your registration. This copy is held electronically in our

records in accordance with the legislation governing the creation of an online gaming account. Given the above, our Company can provide you with a copy of the ID used to create the account. [….]" After completing the verification of the complainant's identity as the actual owner of the police ID in question, using a copy of the mobile phone bill, the OPAP DPO sent her on ... in an encrypted file via e-mail the police ID card that was used in identification box of the user account with the name “ψ”, by sending the decryption key by sms to her mobile phone. At the same time, the DPO informed her that no gambling activity had taken place through the account in question and that, as part of the investigation of the incident, additional information had already been requested from the Agency regarding the identification process followed, for which the 2 complainant would was updated as soon as anything new emerged. It appears from the complaint that it was indeed a copy of the complainant's police identity card. However, the method of obtaining it from the creator of the suspicious account is unknown to her, as she states that she has never visited the mentioned OPAP Agency [region X] and has no relationship with the owner. In her question to the DPO of OPAP, regarding any copy of the DEKO account that should be requested, as required for the identification of an account via the Internet, the complainant was informed that this procedure is not required when the account is identified through an OPAP Agency, as in the case under consideration case. In her subsequent inquiry regarding the progress of the investigation of the case, the complainant on ... was informed that no new information had emerged, and that the contact number on the said account had been stated as ... . According to the complaint, the above proves the existence of a security gap in the Agency account identification process, allowing for "illegal and irregular actions" in the context of achieving sales targets or other illegal actions. of the service of the Terms of Service The Authority, in the context of examining the above complaint against the Agency with store code ... [area X], considering OPAP S.A. as controller and the Agency as processor, in accordance with the mentioned 1st, in articles 1.1, 3.1.2 and 3.1.5, and at the beginning of the section "Information on the Processing of Personal Data" tzoker.opap.gr (https: //tzoker.opap.gr/terms-and-conditions#/), 2nd, in OPAP's Privacy Policy (https://www.opap.gr/gdpr), 3rd, in articles 3.1, 3.1.1 of the Regulation Joker of the E.E.E.P. and 4th, in the definition of the Agency (no. 1) and in article 3.1 of the Regulation of Agents of OPAP S.A. of the E.E.E.P., with no. prot. C/EX/4720-1/11-08-2020 its document, called OPAP S.A. and the Agency in question to state their views, answering in particular the following questions: a) how and why the complainant's police ID copy was used in relation to the user account with the username (username) "ψ", b) whether it was investigated said incident following the relevant protest of the complainant to the company's DPO, and in the affirmative case what is the result of the investigation, and c) what is the

company's policy (OPAP S.A.) for the identification of players as well as whether a certain procedure is to be followed in the event that an incident is reported that 3 raises suspicions of identity theft, fraud, false identification of a player, presentation of falsified identity certificates, etc. The owner of the Agency, B, in his reply from ... (with Authority no. C/EIS/5769/25-08-2020) states that in December 2019, with a specific procedure and instructions, electronic registrations were implemented and customer identification at OPAP Agencies, and within the framework of this Program, registrations were also implemented at its Agency, which is located in a central point [area X], close to the Metro, with the result that its clientele, consisting of 200-250 people daily, don't just limit yourself to the citizens of [area X]. The complained Agent also emphasizes that "the provisions of the Client Registration Procedure at his Agency were strictly observed, where the physical presence of the client at the Agency and the presentation of a police ID card were required". He also states that he reported exactly the same to OPAP S.A., in his letter from ... OPAP SA (hereinafter "the OPAP") with its document from was resubmitted in paper form, first of all it states that following the complainant's verbal and electronic (at the address dpo@opap.gr) requests from ..., on the one hand, to deactivate the suspicious account (with username "ψ") and on the other hand, to provide information and identification documents of the account in question, the customer service department informed the relevant departments (Directorate of Regulatory Compliance and Data Protection Office) of OPAP regarding the message of the complainant who stated that the original account was created without her knowledge, in order to proceed with the relevant investigation of the incident. Subsequently, after the immediate deactivation of the account, on ... the company addressed the Agency, asking for its opinions on the complainants and on ... informed the complainant about the identification process she had to follow in order to send her a copy of the identity card that had been used for the account in question. In this context, OPAP reports on the first question (how and why the copy of the complainant's police ID was used in relation to the user account with username “ψ”) that the suspicious account with username “ψ” was created online with the information of the complainant (name and surname and social security number), and using an e-mail address and phone number, which, as stated itself then, they do not belong to it, and the identification process was then followed, as defined by the regulatory framework governing 4 online gambling. In particular, after creating an online account, it is necessary to "authenticate" it within 30 days, otherwise it becomes inactive. During the 30-day interval, the player can participate in games through their temporary account, but there is a deposit limit of €800 and no winnings can be withdrawn. Thus, in response to the Authority's first question, OPAP states that the copy of the complainant's police ID was submitted for the purpose of identifying the account, on ... to the Agency ..., which, following the

relevant procedure, forwarded to OPAP digital photographs of both sides of said identity. According to OPAP, "no evidence indicated the document's inauthenticity, which was not disputed by the complainant, and the identification was completed." In response to the complainant's allegation that the unknowing use of her ID photocopy demonstrates a security gap, OPAP claims that this is not true because, despite the activation of the account at this stage, in order for the player to proceed with transactions and in particular, in the withdrawal of any amount, identification of the means of payment (IBAN or card details), which are checked by OPAP, must follow, "e.g. confirming with the Bank the details of the beneficiary", as literally stated. According to OPAP, that is, the fact that "the online gaming account cannot be used without further verification of the means of payment of winnings or the e-mail address", in contrast to the provision of other online services, for which it is sufficient to submit a copy identity, demonstrates that even the identification of a player's account through a third party's police ID without their knowledge is not sufficient to establish a "security gap" as it cannot be used in the sense of withdrawing winnings. Furthermore, OPAP maintains that the absence of such a security gap was also confirmed in this case, since the account in question created on ... was never used, while, finally, it also points to the fact that, in addition to its compliance with the security standards of the EEEP, it has and additional, non-mandatory, certifications (ISO/IEC 27001:2013 and World Lottery Association). On the second question (if the incident in question was investigated following the complainant's complaint to the company's DPO, and if so, what is the result of the investigation), OPAP reiterates that it immediately requested the opinions of the Agency and points out that "it is for an event that took place approximately seven (7) months earlier." OPAP reports that it did not receive any further information from the 5 Agency's response, except for the Agent's explicit confirmation that the identification procedures were followed (as is also evident from the Agent's response to the Authority) and that many registrations were made during that period, due to a promotional action, namely providing a €5 bonus to players completing identification, in the form of available balance, for use in games, which was not the case with the suspect account in question. In this regard, OPAP refers to the Agents' Personal Data Processing Policy (ref. 7), which has been sent to all stores since 2018, is posted on the portal ..., the agency's communication platform with the company, which is visited daily by everyone the Agents, and, as follows from article 3 of the Agency contract (ref. 8), it is a legally binding part of the Agents' contract with the company. OPAP also notes that the mobile phone number that had been declared was not active, nor did its search in publicly accessible phone books yield results. Regarding the third question, (what is the company's policy for the identification of players as well as whether a certain procedure is to be followed in the event that an incident is reported that raises suspicions

of identity theft, fraud, incorrect player identification, presentation of falsified identity certificates, etc.) OPAP, focusing on the process of identification of players through a store, attaches and cites internal documents describing the relevant procedures, which it claims were followed in this case as well. Specifically, OPAP provides the description of the "Online Player Verification Process - Verification through Retailer" (ref. 9 - in English), the Instructions to Agencies for the Step-by-Step Identification of a New Player (ref. 10) and the regular control process from the Antifraud department (i.e. fraud prevention, ref. 11 – in English) and states that "the Data Protection Office promptly handled the complainant's access request, completing the identity check, responding to the requester in a timely manner and securely sending all the information and information requested. The Agency Support Department, in collaboration with the Regulatory Compliance Division and the Data Protection Division, forwarded the complaint, requesting an explanation from the Agency. The agency's response, combined with the available evidence, was reviewed by the Division of Regulatory Compliance, which responded with a strong recommendation to comply with the identification rules." It is noted that at another point, OPAP 6 states that "it has compliance control procedures for its agents, which may result in recommendations, the imposition of sanctions or even the termination of the contract, if their non-compliance is found". In conclusion, OPAP points out that "no damage was caused to A, given that even if a third party gained access to her information (which cannot be inferred from anywhere that it can be related to or due to the company or the Agency) in any case no transaction was carried out through the gaming account created with the above procedure". Subsequently, the Authority, with no. prot. C/EX/4720-2/28-12-2021 in her document, on the one hand, she asked OPAP to clarify, in what way the documents she presents in relation to 9-11 (instructions, procedures and policies) are communicated to the Agents and if it is confirmed that they are aware of them, as well as if in this case it found non-compliance by the Agency - performing the processing, on the other hand by B (Agent) to clarify whether the ... action invoked also covered the date ... on the which the critical registration allegedly took place and if the identification in this case at the Agency was done with the physical presence of a person who bore the identity of the complainant. In his reply document dated ..., the Agent gave an affirmative answer to both of the above answers, pointing out that due to the passage of a long period of time and due to the large number of identifications during that period, he is unable to specifically recall the specific case of the complainant's identification, stating, however, that customer identification was invariably done by physical presence and identification. With its letter from … OPAP replied that only the document submitted as Relevant 10 (Instructions for New Player Identification Step by Step) is shared with the Agents by posting on their training platform …, that no confirmation is requested from the

Agents that they have received knowledge of the material posted, however when new educational material or new procedures are created, the Agents are informed by announcement through the platform, and any failure of the Agent to be informed would constitute a breach of its contractual obligations and would make the operation of the Agency difficult and impossible to complete of the online identification process. OPAP maintains that in this case the Agent submitted the documents to the system in the manner specified in the above Instructions, which confirms that he has taken note of them. Finally, OPAP states that from the control of the 7th Agency that it carried out in the context of examining the complaint in question, it did not find insufficient compliance, however, taking into account the claims of the complainant, it cannot rule out the possibility that the control of similarity was not sufficiently diligent of the person who presented the identity card with the complainant's photo on the identity card. In the absence of more evidence, OPAP maintains that it is not in a position to assess whether the check was indeed flawed or whether it was a third person who, due to the similarity, could reasonably be considered to be depicted on the identity card, nevertheless it considered that it should have pointed out to the Agent the need to comply with the rules of identification through a strict recommendation, without this having the meaning of sanction, but as a warning and reminder of the rules that apply. Subsequently, the Authority, with no. prot C/EXE/966/31-03-2021 and C/EXE/967/31-03-2021 calls to a hearing by video conference to the complainant and the accused (OPAP S.A. and B) respectively, invited the involved parties to a hearing at the meeting of the Department of the Authority on 04/07/2021, in order to present their views on the case. During the hearing, the parties developed their views and were given a 10-day deadline to submit briefs. During the hearing of 04/07/2021, the complainant, the attorneys of the controlled company OPAP S.A., Apostolos Vorras (…) and Konstantina Karopoulou (…), and the attorney of the complainant B, Mr. Vasilios Tsiatis (...). OPAP S.A.'s C, YPD were also present. and D, an employee of the OPAP Data Protection office, who did not receive the floor. The parties involved were given, during this meeting, a deadline and submitted in a timely manner, while defendant B with no. prot. G/EIS/2651/19-04-2021 memorandum, and the audited OPAP with no. prot. C/EIS/2652/19-04-2021 memorandum, while the complainant did not file a memorandum. The complainant referred to her complaint during the meeting. The complained Agent OPAP B, both during the meeting of 04/07/2021 and with his memorandum, argued that his Agency, which is located in a very central point [area X] and receives about 200 visitors daily, is a fast growing business, which takes care of the continuous training of its employees so that all the conditions for its legal operation are met. At the same time, the Agency actively participates... The completion of the process of creating the 8 account required the identification of the customer through his

presence in person at an Agency and the presentation of his original police ID, which is then scanned on the special OPAP computer by the respective agent. At this point it is worth noting that the complainant mentions in his memorandum the following: "The process of identifying the users who came to my business consisted of two necessary stages without strict observance of which it could not be completed. It was specifically required that j) the person concerned should come to the agency in person and indicate his access details (username and password) so that we could gain access to his account where his personal details were (such as phone and contact address) and ii) show the agent his original police ID. The agent then placed the identity card in front of OPAP's special computer inside the agency so that a digital copy of it (scan) could be taken through the camera integrated in it." Furthermore, according to the complainant, the identification of the complainant was made at his Agency on …, during a period of particularly increased mobility and clientele due to the local flea market which took place on the same day right next door, but also due to the consecutive JOKER jackpots which resulted in potential profits amounting to 4 million euros. Thus, as stated by the complainant, the identification process by the Agency employees could not be extremely detailed, but was limited to the formal comparison of the person who appeared before them and the original police identity card shown to them, with which discrepancies were quite often observed due to age of the photo or due to scratches on the ID. Consequently, the complained Agent claimed that he would not be able to check and even realize whether a third party used the complainant's identity to identify the OPAP account created in her name. Furthermore, the complainant stated that, for reasons of personal data protection and after the lapse of more than 1.5 years, he has not kept records of the persons who, through his Agency, identified their electronic accounts on the OPAP platform for JOKER, and thus he is not in a position to have an exact picture of the number of identifications carried out by his Agency, however he roughly states that this number did not exceed 95 persons and is very small compared to the capacity of his business. ..., he had no reason to risk his professional credibility and his contract with OPAP, by violating the personal data of customers. Finally, according to the 9th account of the complaining agent, it was never used, so as to result in any financial burden, while six months after it was opened, it was deactivated. In support of his allegations, the complainant submitted his 2019 tax year statement, which shows the size of his business (approximately ... gross revenue and ... profits) and requests that the complaint be dismissed. OPAP, during the meeting of 04/07/2021, through its representative, after briefly referring to the history of the case, argued that it was a case of identity theft, which, however, did not cause damage to the complainant thanks to its security valves OPAP identification system. Responding to relevant questions from the Authority, the representative of

OPAP stated that the identification of a player in an Agency is only allowed with the full ID of the person appearing and not with a photocopy, while he speculated that the third party who could carry out such an action could is either a minor or a banned player. Subsequently, with its memorandum of 19/04/2021, OPAP in principle referred to the two documents with which it provided its opinions (G/EIS/5824/28-08-2020 and G/EIS/252/13-01 -2021) following the respective requests of the Authority. Presenting the full text of the Agents' contract, which is applied uniformly throughout the territory, OPAP stated that after the implementation of the GDPR the terms of personal data protection were modified and their processing is now governed by the Policy on the Processing of Personal Data by OPAP Store Agents , which has been submitted to the Authority as Rel. 7 of OPAP's letter dated 27.08.2020, pointing out that on ... a basic term of the contract in question was modified, ... Responding to a related question from the Authority, OPAP noted that following an investigation, another case was found in which a player started his registration on ... 2021 via the internet and was unable to complete it due to the existence of an account in his name and with his identity information, which had also been established in Agency [region X] under no. …. Although the player was asked to send some contact information to confirm the incident, he did not respond or get back. However, OPAP again sent a letter addressing a strict recommendation to the Agency, with the warning of sanctions in case of a new complaint or established violation. Furthermore, with its memorandum, OPAP clarifies the concept of a fake account, as it was requested in the context of the hearing, citing 10 specific examples. OPAP then lists some information covered by business confidentiality, with the request that they not be shared, ... At the same time, there was an offer of €5 for every player who would register with the Agency, either through the OPAP application or through tzoker.gr. OPAP points out again that it has taken all the necessary technical and organizational measures to protect the players, since even if there is a malicious action, it is not possible to use the account and withdraw amounts if identification through a bank is not followed, citing in support of the claim of that although approximately ... players have registered online by entering their details, and the players who have completed their identification amount to ..., however, the only complaint that has taken place in the aggregate of so many thousands of players is the particular one under consideration by the Authority, a fact which demonstrates the safety and effectiveness of its procedures. Finally, OPAP states that the creation of fake online accounts by a third party causes damage to OPAP, since on the one hand it pays Agents fees for non-revenue players, on the other hand in case the prospective player finds that the details have already been used of him, this ultimately acts as a deterrent and thus he does not proceed with his registration and online participation in the games of chance, as happened in the case of the complainant as well as that the said complaint

is not against OPAP. The Authority, from the hearing procedure, from the elements of the case file, as well as from the memoranda submitted to the Authority and after hearing the rapporteur and the assistant rapporteur, who left after the discussion of the case and before the conference and the taking a decision and after a thorough discussion, IT WAS CONSIDERED IN ACCORDANCE WITH THE LAW 1. From the provisions of articles 51 and 55 of the General Data Protection Regulation (Regulation (EU) 2016/679 - hereinafter, GDPR) and article 9 of law 4624/2019 (Official Gazette A' 137) it follows that the Authority has the authority to supervise the implementation of provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 2. According to the definition of article 4 no. 2' GDPR as "processing" means "any operation or series of operations carried out with or without the use of automated 11 means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction". Furthermore, as defined in Article 5 para. 1 GDPR ("Principles governing the processing of personal data") "personal data shall be processed in a manner that guarantees the appropriate security of personal data, including its protection from unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")'. Furthermore, according to Article 6 GDPR, "the processing is lawful only if and as long as at least one of the following conditions applies: a) the data subject has consented to the processing of his personal data for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary to comply with a legal obligation of the controller , d) the processing is necessary to safeguard a vital interest of the data subject or another natural person, e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of public authority assigned to the controller, f) the processing is necessary for the purposes of legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child". In addition, according to Recital 40 of the GDPR, "In order for the processing to be lawful, personal data should be processed based on the consent of the data subject concerned or on another basis, provided by law, or in this Regulation or in other Union legislation or regulation, including the need to comply with the statutory obligation in the Member State as referred to in this 12 3. to which the controller is subject or the

need to perform a contract to which the data subject is contracting party or to take steps at the request of the data subject prior to the conclusion of a contract'. The GDPR mandates the submission of personal data for processing "in a way that guarantees appropriate security ... including their protection against unauthorized or illegal processing and accidental loss, destruction or damage using appropriate technical or organizational measures" (Article 5 par. 1 par. f and 32 par. 2) so that in a case where the other principles are met except that of security, the processing ultimately becomes illegal. Taking the required security measures must take into account a number of parameters (see article 32 GDPR) while as mandated by the principle of accountability and determined by the provisions of article 24 par. 2 GDPR, appropriate policies must be applied, depending on the activities processing (see APDPX 67/2018). Furthermore, according to Article 28 para. 1 GDPR, "When the processing is to be carried out on behalf of a data controller, the data controller shall only use processors who provide sufficient assurances of the application of appropriate technical and organizational measures, in such a way that the processing meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Paragraph 3 of the same article clarifies that the processing by the processor is governed by a contract or other legal act, subject to the law of the Union or the Member State, which binds the processor in relation to the controller and defines the object and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller. The said contract or other legal act provides in particular that the processor processes the personal data only on the basis of recorded instructions of the data controller, takes all the required measures pursuant to article 32 GDPR. According to Article 32 para. 1 GDPR "Taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the 13 4. 5. controller and the processor implement appropriate technical and organizational measures in order to ensure the appropriate level of security against the risks [...]'. According to the consideration no. 127 of the Guidelines under no. 07/2020 of the GDPR on the concepts of controller and processor in the GDPR, “[…] the level of instructions given by the controller to the processor as to the measures to be taken depends on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented or, in other cases, may describe the minimum security objectives to be achieved, while asking the processor to propose the implementation specific security measures. In any case, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as the

approval of the measures proposed by the processor." 6. In this case, from the information in the file and from the hearing, the following emerged: On ... a temporary online account was created on the website https://joker.opap.gr by an unknown person with the identity information of the complainant (name, surname and social security number), without her knowledge, with the username "ψ" and using an e-mail address and phone number, which have nothing to do with the complainant. Given that the completion (finalization) of online account creation requires the identification of the customer through his/her presence in person at an Agency and the presentation of his/her original police ID, which is then subjected to digital photographic processing (scanning) through OPAP's special computer by the each agent, it emerged that on the same day the above procedure was followed in the complained Agency [area X]. The owner of the Agency, B, and who performs the processing on behalf of OPAP, in his reply to the Authority from ... (with Authority No. C/EIS/5769/25-08-2020) states that in the present case " the procedures for the registration of customers at the Agency were strictly observed, where the physical presence of the customer at the Agency and the presentation of a police ID card were required". He also states that he reported exactly the same to OPAP S.A., in his letter from ... And the relevant procedure is described in the Form of Instructions to the Agencies for the Identification of a new player 14 Step by Step, which OPAP presented as Related 10 with its opinion document from ... (prot. no. C/EIS/5824/28-08- 2020 and C/EIS/5852/28-08-2020), answering a relevant question from the Authority regarding the company's policy for the identification of players, claiming that this procedure was also followed in the case of the complainant. This form includes the following New Player Identification Steps: … Furthermore, as stated in the OPAP Store Agent Data Protection Policy (Ref. 7, attached to C/EIS/5824/28-08-2020 OPAP opinion document), "3.3 The Agent should in any case process Personal Data only in accordance with OPAP's recorded instructions (as included in this Policy or as sent from time to time by OPAP) and only for the purposes of the Agency Agreement or as specifically defined in said instructions […], 3.4 […] c) The Agent , taking into account the type of Processing it performs and the information it has, will help OPAP comply with its obligations arise from the Applicable Legislation, such as the obligations concerning: - The security of the Processing, in accordance with article 32 of the GDPR". As it appears, therefore, OPAP, in its capacity as data controller, assigns through a contract to the Agents, in their capacity as processors, to carry out the identification process of players who create an account on the joker.opap.gr page, providing specific and recorded instructions "step-by-step" to be followed by the Agents for said processing. 8. The complained Agent in the views he submitted to the Authority (G/EIS/135/08-01-2021) argued, among other things, that for the identification of all customers, he followed the Procedure regarding physical presence

and demonstration of their police identity cards, while with his hearing memorandum (G/EIS/2651/19-04-2021) stated that this was "a time of particularly high traffic and clientele visiting his Agency" due to the local [area X] flea market taking place on the same day right next to his business, but also because of the back-to-back jackpots of JOKER, which resulted in potential profits amounting to 4 million euros. Thus, as he stated, "under the given circumstances of the large number of clients coming to my agency, the identification process received by [country] in the context of ... (both by me as an administrator and by my 15 employees) could not be extremely detailed – since we are not a public authority – but it was limited to the formal comparison of the person presented before us and the original police ID that he showed us. However, this comparison is not an easy process, especially under conditions of intense mobility in my agency...", while according to him, quite often mismatches were observed due to the age of the photo or the comparison was difficult, due to tears or abrasions on the ID, pointing out that the identity in question in the case of the complaint was issued in the year 2006. Consequently, the complained Agent claimed that "neither he personally nor the staff of his agency could check and even perceive if any third person came to the agency and proceeded, instead of the complainant, to identify the corresponding account (with the complainant's details) in OPAP using the original identity of the complainant". 9. In this case, the digital photographing of the identity card presented to the complaining Agency and identical to the identity card of the complainant as well as the registration of its electronic digital copy in the OPAP system constitutes processing (collection and registration) of the personal data of the complainant carried out by automated means, according to the definition of article 4 no. 2' GDPR. Such processing takes place only under the condition of the assistance of one of the legal bases of Article 6 para. 1 GDPR, in compliance with the processing principles of Article 5 para. 1 GDPR. For the correct application of the required legal basis and for the legal processing of personal data no. 5 par. 1 sec. a' GDPR in this case it is assumed that the identity of the displayed person is confirmed at the Agency where he must present his identity card in order to create an account. The legal basis of the processing is determined by OPAP, in the capacity of the controller, while the identity control is assigned to the Agent, in the capacity of the processor based on the explicit and recorded orders no. 28 GDPR, in compliance with the Policies established by no. 24 and 32 GDPR the OPAP. If the candidate for the creation of a customer-player account presents to the OPAP Agency a card with identification-legitimizing identity details of another data subject and pretends that he is depicted on the identity card by making use of the identification-identification details, then the processing of personal data 16 is carried out without the existence of a legal basis under no. 6 par. 1 GDPR and consequent violation of the principle of legality according to

no. 5 par. 1 sec. 1 GDPR, regardless of the fact that the Agent was unaware of the fact that the person appearing before him was not the person depicted on the identity card due to having carried out a faulty identity check, as will be demonstrated below. 10. In the case of the present complaint, it emerged that the incorrect identification of the person appearing before the OPAP Agent is primarily due to the faulty control that he admits in this case that he applied as the executor of the processing, due to the conditions of high customer mobility at the Agency of those days, as ... . In particular, as the Agent himself specifically stated “[…]”under the given circumstances of the massive influx of clients to my agency, the identification process received by [country] in the context of … could not be extremely detailed – since we are not a public authority – but it was limited to the formal comparison of the person who was presented in front of us and the original police ID that he showed us"... However, this comparison is not an easy process (especially under conditions of intense mobility in my agency...". In view of the above, the Authority finds in principle that the large number of incoming customers to be registered ("bulk" according to the agent) resulted in said identity verification being carried out without the appropriate and required patience, care and diligence, but instead with the maximum possible speed in order to serve all customers as quickly as possible.This faulty control by Prak therefore resulted in the lack of identification not being established and the processing of the complainant's personal data taking place by digitizing a copy of her police ID and creating an initial account at OPAP, without the complainant's knowledge and without any of the legal bases of article 6 par. 1 GDPR. The aforementioned faulty control constitutes a violation of the obligations of the alleged processor under Articles 24 and 32 of the GDPR to comply with the instructions of the data controller to implement the appropriate technical and organizational measures during the identification process (cf. APD 140/2017 for the case of incorrect identification and violation of personal data), since as it is found, the written Instruction of Step 2, referred to in number 3, included in the form of Instructions to Agencies for the 17 Identification of a new player Step by Step, which OPAP presented as Relevant 10 with his opinion document dated 26-08-2020 (prot. no. C/EIS/5824/28-08-2020 and C/EIS/5852/28-08-

2020), according to which the Agent must "ensure that the document corresponds to the natural person and the document presented by the customer". Besides, there is another inconsistency in the actions that the complained Agent stated that he applies during the process of identifying players in his store in relation to the explicit Instructions of the OPAP controller. In particular, as stated verbatim in the complainant's memorandum (G/EIS/2651/19-04-2021, p. 4): "The identification process of the users who came to my business consisted of two necessary stages without strict observance of which could be completed.

It was specifically required that j) the person concerned should come to the agency in person and indicate his access details (username and password) so that we could gain access to his account where his personal details were (such as phone and contact address) and ii) show the agent his original police ID. The agent then placed the identity card in front of OPAP's special computer inside the agency so that a digital copy of it (scan) could be taken through the camera integrated in it." However, indicating the player's credentials (username and password) to the Agent is not included in the "Step-by-Step Instructions" received by the processing Agent for the identification of players in a store (ref. 10 in no. C/EIS /5824/28-08-2020 opinion document) while it appears particularly problematic from a security point of view (risk of loss of data confidentiality). Finally, from the documents in the file, it was established in this case that OPAP was unaware that the Agent was applying an identification procedure different from the one included in the instructions he provided as data controller, as well as that no sufficient control of the application of the provided identification instructions. 11. Based on the above, the Authority finds that the processing Agent of OPAP improperly applied the identification procedure set by the OPAP data controller, while the OPAP data controller did not carry out the necessary checks to ensure the correct application of identification ofof data subjects in accordance with the instructions he provided.

18

Following the above, the Authority finds:

a) violation of article 6 par. 1 GDPR and no. 5 par. 1 sec. a' GDPR of principle
legality, due to the lack of a legal basis for the processing of personal data
data of the complainant, due to the faulty identity check which
performed by the complained Agent as a processor on its behalf
OPAP data controller and

b) violation of articles 5 par. 1 sec. first cond. f, 24 and 32 GDPR which impose the
application of the appropriate technical and organizational measures for correct identification –
authentication of the data subject by the processor
based on the instructions of the controller.

12. In accordance with the GDPR (see p. s. 148) in order to strengthen the enforcement of the rules
of this Regulation, sanctions, including administrative fines,

should be imposed for each violation of this Regulation, additionally or

instead of the appropriate measures imposed by the supervisory authority pursuant to

this Regulation. In cases of minor violations or if the fine

likely to be imposed would constitute a disproportionate burden on a natural person,

a reprimand could be imposed instead of a fine.

Based on the above, the Authority considers that there is a case to exercise the following

article 58 par. 2 of the GDPR its corrective powers in relation to the established

violations, without having to impose under no. 83 GDPR administrative fine for

restoration of compliance with the requirements of the GDPR, taking into account

circumstances of the specific case, the fact that the controller had

take the necessary measures so that the opening process is not completed

account and that no further processing operations are subsequently carried out

personal data but neither to transact money online

game.

You should therefore according to the above:

i.

To address warning no. 58 par. 2 sec. GDPR to the person in charge

OPAP processing in order to carry out checks and effective countermeasures to

processing Agents in order to ensure that on their part

compliance with the instructions for identifying potential customers - players.

19

ii.

To address to the processor Agent B a reprimand according to art. 58

par. 2 sec. b GDPR for violation of articles 6 par. 1, 5 par. 1 sec. first cond. f', 24 and 32

GDPR due to the processing of the complainant's personal data without her

existence of a legal basis and in case of improper compliance with the identification procedure.

Based on the above, the Authority unanimously considers that it should be imposed on OPAP as

data controller and to the denounced Agency as the executor thereof

processing or referred to respectively in the administrative sanction, which is judged

proportional to the gravity of the violation.

FOR THOSE REASONS

THE BEGINNING

It addresses the OPAP controller with warning no. 58 par. 2 sec. 1 GDPR

in order to carry out checks and especially more effective ones on those performing it

Processing Agents in order to ensure their compliance with

instructions for identifying potential customers - players.

Addresses to the processor Agent B a reprimand according to art. 58 par. 2 sec. b'

GDPR for violation of articles 6 par. 1, 5 par. 1 sec. first cond. f, 24 and 32 GDPR due

processing the complainant's personal data without the existence of a legal basis

basis and for failing to comply with the identification procedure.

The Deputy President

George Batzalexis

The Secretary

Irini Papageorgopoulou