Athens, 01-10-2021 Prot. No.: 2198 DECISION 43/2021 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via video conference on 19-

07-2021, in order to examine the case referred to in the history of the present. Konstantinos Menudakos, President of the Authority, regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, and Charalambos Anthopoulos were present. At the meeting, without the right to vote, the auditors Konstantinos Limniotis and Spyros Papastergiou, IT specialists, were present, as assistants to the rapporteur, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary, by order of the President. The Authority took into account the following: The written report of A was submitted to the Authority with original number C/EIS/7897/17-11-2020, in which the following are mentioned: a) On …/2020 he sent an email to Hellenic Police, and in particular at the address …@astynomia.gr, which included his personal data such as, in addition to his electronic address, his name and personal code for the Passenger Location Form service, regarding his visit to Greece on … of 2020. b) Subsequently, without receiving a response from the Hellenic Police, he received four different electronic messages which "pretended" to be from the Hellenic Police and either contained malware or links that referred to malicious software (the messages Ave. Kifisias 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 are attached to his above reference). As the complainant specifies, the Internet addresses (IP addresses) from which the messages in question allegedly originate correspond to various countries abroad (specifically, Y, F, X and Y). From the said messages it appears that the complainant's original message to the Greek Police has been leaked entirely to unknown third parties. c) In a telephone call he had with the Greek Police on …/2020, a representative of the Service informed him that there was a security problem with his e-mail. d) The above is described by the complainant in an email message he sent to the Hellenic Police on …/2020, in which he also requests the position of the Hellenic Police on the incidents in question (and which was communicated to the Authority with the above his reference). Subsequently, with his document No. G/EIS/8192/30-11-2020, the complainant informed about a named posting on the Internet of another person to whom, according to his claims, exactly the same thing happened (the link is The: …). Following the above, the Hellenic Police forwarded to the Authority with its document no. complainant in his above request. In particular, in the reply in question (with prot. no. … and date …2020) it is described that on the dates of receipt of the aforementioned four e-mails from an alleged sender of the Hellenic Police, a cyber attack with the code name “EMOTET” was in full progress which manifested globally. Furthermore, from the study of the code of the said messages (which was also included in the complainant's initial letter), it

appears that the messages were not sent from the infrastructure of the Hellenic Police but from electronic accounts that have nothing to do with the Hellenic Police (and which are listed in said document). Subsequently, the complainant forwarded to the Authority, with his document No. C/EIS/487/19-01-2021, No. … and from …2020 document 2 of the Hellenic Police, with who had been informed, by the Data Protection Officer of the Hellenic Police, that his request had been forwarded to the IT Security and Personal Data Protection Department of the IT Directorate of the Hellenic Police (the document in question was the initial response from the Hellenic Police , to his request, before the final reply with the aforementioned letter dated …2020). Following the above, the Authority sent the Greek Police the document No. C/EXE/482/27-01-2021, with which it invited it to describe the exact actions it took to verify the safety of the of its systems in relation to the matter in question, considering that, although it is clear that the messages in question were not sent by the Greek Police, it did not appear from its reply to the complainant that a check was carried out on its part if any of its subsystems (e.g. workstation) has been "infected" by malicious software or if its security has been breached in any other way, so as to "facilitate" the spread of the above cyber-attack. In the same document, the Authority pointed out that such a check is an obligation of the Greek Police, given that on the one hand the aforementioned malicious messages contained the same text that had already been processed by the Police's e-mail applications, and on the other hand that the aforementioned cyber-attack is based, for its spread, in malicious software that is installed in e-mail programs (referring to a text of the European Cybersecurity Agency (ENISA)1), as well as that, in a case where there has been a breach of security under the system of the Hellenic Police, then – in addition to the obligations to promptly deal with it and restore security – the provisions of articles 33 and 34 of the General 1 See the relevant ENISA report for 2020: https://www.enisa.europa.eu/publications/malware as well as the related reports there. 3 of the Data Protection Regulation regarding personal data breach incidents. In response to this, the Hellenic Police (Information Security and Personal Data Protection Department of the IT Directorate) submitted to the Authority the no. prot. … and from …/2021 its response (authority prot. no.: Γ/ΕΙS/1162/17-2-2021), in which it mentions the following regarding the actions it took regarding the incident in question: a) Initially, the possibility of penetration or infection of the organization's servers was investigated by Service officials, in cooperation with the support contractors of the specific systems, without establishing any violation. b) In addition, in order to limit the transmission of EMOTET, the organization took the following organizational and technical measures: i) for intermediate mail relays: the antibiotic, spam and malicious content filtering rules were strengthened, some mail domains were "blacklisted" and senders, additional keyword filters were created on message content, while the latest

system software updates were installed, ii) for email servers: antibiotic, spam and malicious content filtering rules were strengthened, although they cause more misidentifications, iii) for workstations: format was done in four isolated cases where infections were found, older versions of MS Outlook were upgraded (where used), regional administrators checked for out-of-date antibiotic software and ensured that it was updated, all checked the operator's workstations for possible detection of harmful messages, changed the password (password) of some users and requested the use of webmail instead of MS Outlook, 4 implemented changes in the domain policies to limit execution rights of applications, macros and powershell, iv) for the informing end users: an information document was circulated through an internal mail application informing users about the wave of malicious spam messages, how to handle them and who to inform, v) to inform competent authorities: the national CERT, the Cybercrime Prosecution, the Data Protection Authority and affected organizations due to their senders. The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteurs, who (assistants) left after the discussion of the case and before the conference, after a thorough discussion OLD IN ACCORDANCE WITH THE LAW 1. According with the provisions of articles 51 and 55 of the General Data Protection Regulation (EU) 2016/679 (hereinafter, GDPR) and article 9 of Law 4624/2019 (Government Gazette A

137), 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 Article 4 of the GDPR, a data controller is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of processing personal data; when the purposes and method of processing of which are determined by the law of the Union or the law of a Member State, the controller or the special criteria for his appointment may be provided by the law of the Union or the law of a Member State", while the processor is defined as "the natural or legal person, public authority, agency or other body that processes personal data 5 on behalf of the controller". In this particular case, the controller within the meaning of Article 4 of the GDPR is the Greek Police. 3. In the same Article 4, a personal data breach is defined as "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed" . 4. According to article 5 paragraph 3 of the GDPR the data controller bears the responsibility and must be able to demonstrate compliance with the processing principles established in paragraph 1 of the same article (including confidentiality and data integrity according to article article 5

paragraph 1 letter f'). In other words, with the GDPR, a compliance model was adopted with the central pillar being the principle of accountability in question, i.e. the controller is obliged to design, implement and generally take the necessary measures and policies, in order for the data processing to be in accordance with the relevant legislative provisions and, in addition, must prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 5. Pursuant to Article 24 para. 1 of the GDPR, the controller, taking into account 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 the natural persons, implements appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR, while also these measures are reviewed and updated when deemed necessary. Furthermore, according to Article 32 of the 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 liberties of natural persons, the controller and processor implement appropriate technical and organizational measures in order to 6 ensure the appropriate level of security against risks, including, among others, as appropriate: (…) d) procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing". Furthermore, in paragraph 2 thereof, it is stated that "when assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed'. 6. With regard to personal data breach incidents, the GDPR defines specific obligations for data controllers. Specifically, in article 33 thereof, it is defined that in the event of a personal data breach, the data controller shall notify the competent supervisory authority without delay and, if possible, within 72 hours of becoming aware of the personal data breach2, except if the breach of personal data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay. 7. Paragraph 3 of article 33 defines the information that must be contained as a minimum in such a notification, which includes - among others - the potential consequences of the breach of personal data, as well as the received or proposed to be received measures by the data controller to deal with the personal data breach, as well as, where appropriate, measures to mitigate its potential adverse consequences. In the event that it is not possible to provide the information at once, it may be provided gradually without undue delay. 2 Taking into account article 55 of the GDPR on the powers of the supervisory

authorities, the Personal Data Protection Authority is responsible for the incident in question. 7 8. Furthermore, in accordance with Article 34 of the GDPR, when the personal data breach may put the rights and freedoms of natural persons at high risk, the controller shall promptly notify the personal data breach to the data subject. This notification clearly describes the nature of the personal data breach and contains at least the information and measures referred to in Article 33(3)(b), (c) and (d). Notification to the data subject is not required if any of the following conditions are met: a) the controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach, in particular measures that make it unintelligible the personal data to those who do not have permission to access it, such as encryption, b) the controller has subsequently taken measures that ensure that a high risk to the rights and freedoms of the data subjects is no longer likely to arise, c) requires disproportionate efforts (in which case a public announcement is instead made or there is a similar measure by which data subjects are informed in an equally effective manner). 9. Pursuant to article 12 par. 1 of the GDPR, the data controller shall take appropriate measures to provide the data subject with any information referred to in articles 13 and 14 (which concern the information provided to the data subjects or the data is collected from the subjects themselves or not) and any notice under Articles 15 to 22 (which concern the rights of data subjects, including the right of access in Article 15) but also the aforementioned Article 34 regarding processing, in a concise, transparent, understandable and easily accessible form. In particular with regard to the right of access of Article 15 of the GDPR, the data subject has the right to receive from the data controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, access to any information about processing. 8 10. In this particular case, it is a cyber security incident which took place at a global level and has been named as EMOTET3 affecting a number of operators. This incident is linked to the spread of malware. According to a statement by Europol on 27/1/20214, the malware in question is installed on victims' workstations via "infected" file attachments in e-mail messages, which in order to mislead their recipients appear in various ways, such as allegedly proof of payment or information about COVID-19. The infected files attached were of the Word type, which upon "opening" prompted the user to activate macros, which in turn allowed the malware to be installed on the victim's workstation. In the same Europol announcement, there are ways in which one can generally deal with this type of attacks like that of EMOTET, which are based on a combination and updated operating systems) and vigilance of users not to "open" suspicious attachments. cyber security (antibiotics tools software 11. If a cyber security attack has resulted in a breach of personal data, then it is - according to Article 4 of the GDPR - also an incident of

personal data breach. This seems to be the case in this case, according to the initial report of the complainant but also with the nature and characteristics of the attack 5. 12. For this specific case, there was no notification of the said incident to the Authority as required by article 33 of the GDPR. It is noted that there are clearly risks - indeed high - for the affected persons and, therefore, the incident in question does not fall under the exemption from the obligation 3 It is the name of the relevant botnet.4 See https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

5 To this end, it should be noted that, in the aforementioned Europol announcement, it is stated in particular that following the actions of the Dutch Police, a database with information such as email addresses, user names and passwords, which were leaked in the context of the EMOTET attack, where one can see if his details have leak out.

of its disclosure, precisely because of the fact that electronic messages mail "pretend" that they have the Greek Police as the sender (and so, a bona fide recipient of them with no security experience, will could "open" them), while moreover the content of the messages contains information – including personal data – that existed in previous legitimate e-mails, so it is born issue of unauthorized access and dissemination of data which citizens submitted to the Greek Police. Yes, in this particular one in this case, there may also be a question of violation of her privacy communication, which is a fundamental right according to article 19 of the Constitution and Article 7 of the EU Treaty, which reinforces the claim of high risks from the incident in question. Even if it is considered that, after the attack EMOTET became widely known, it took time to investigate and to

clarify whether it is indeed an incident of personal violation

data for the body, the content of its relevant report

complainant demonstrates a high probability of such a case and therefore,

the Greek Police as data controller should have investigated immediately

The incident. After all, as it turned out, they were indeed "infected"

workstations within the controller, the existence of which

contributed to the successful attack (because otherwise, if no one had been hurt

subsystem of the Hellenic Police, the said incident would not concern

the Greek Police as controller6).

While the Greek Police, in its latest document to the Authority, states

that, in the context of dealing with the incident, he informed the Authority, such

there was essentially no information (since the only information was its transmission

of her reply to the complainant, which reply indeed – as

analyzed below – did not have complete information).

6 E.g. a general sending of non-genuine e-mails impersonating their sender

the Hellenic Police, does not constitute a security incident for the Hellenic Police if the mission

this is not based on a hit to any subsystem of the Hellenic Police.

13. In addition to not reporting the incident to the Authority, there was also no

informing the affected persons, in accordance with article 34 of the GDPR. Due to

of the high risks arising from the incident in question, such as

analyzed above, it follows that such an update was mandatory.

Besides, according to par. 3 of the same article, if the information of

affected persons cannot be carried out because it presupposes

disproportionate efforts (something that could probably be documented

for the case in question, due to the peculiar nature of the incident), then

a public announcement is made instead or a similar measure is taken whereby

data subjects are informed in an equally effective manner.

It does not appear in this particular case that such a general action took place

character update.

14. It is also pointed out that the information provided by the Greek Police to

complainant (see above), in the context of his request which is

special manifestation of the right of access, cannot be considered as

complete, since they are limited to reporting that the messages, which he himself

received, do not come from the Greek Police and are part of the framework

of the cyberattack under the name EMOTET, without describing that the

Greek Police has taken appropriate actions to deal with it.

Essentially, from the response of the Greek Police to the complainant

it does not clearly appear that there was a security incident for Hellenic

Police, from which his personal data was breached.

15. In its latest document to the Authority, the Greek Police describes

set of actions taken to investigate the incident. Sit down

these actions seem to be in principle in the right direction, however

it does not appear that the possible consequences of the incident were thoroughly investigated

(e.g. it was not investigated how many persons there was a data leak, as

also what kind of data this was), with the result that the

relevant assessment of the consequences - which was mandatory under the

as defined in articles 33 and 34 of the GDPR. Further, it does not arise with

clarity that the measures in question – although, as mentioned above, are clearly in

right direction - were adopted after analyzing the risks for the

specific case (i.e. no specific documentation of it is listed

appropriateness and completeness of the measures in view of the risks involved

face). Finally, it follows from these actions that they existed

cases where operating systems or antibiotics had not been updated

software, and this omission demonstrates a generally significant deficiency

procedures for updating and reviewing security measures (this applies

regardless of whether said failure to update contributed to said event

data breach or not).

16. The Authority, taking into account the above found violations of the articles

32, 33 and 34 of the GDPR regarding the security of processing, but also of

of article 15 of the GDPR regarding the completeness of the response to a right

of access, and taking into account the size of the cyberattack on the one hand

EMOTET which is known to have infected a very large number of systems

around the world and on the other hand that the controller has taken actions

to deal with it and to prevent a corresponding future attack,

deems that the conditions for enforcement against him are met according to article 58

par. 2 b' of the GDPR administrative sanction, as stated in its operative part

present, which is considered proportional to the gravity of the violations.

FOR THOSE REASONS

The beginning,

Addresses to the Greek Police, as controller, reprimand for the

as above found violations of articles 32-34 and 15 of the GDPR.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou