Athens, 11-08-2020 Prot. No.: G/EX/5588/11-08-2020 GREEK REPUBLIC PERSONAL DATA PROTECTION AUTHORITY A P O F A S I NO. 27/2020 The Personal Data Protection Authority met in its headquarters on 30/7/2020 at 10:00 a.m. upon the invitation of its President, in order to examine the case referred to in the history of this present. The President of the Authority, Konstantinos Menudakos, and the regular members of the Authority Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, and Charalambos Anthopoulos were present. The meeting was also attended, by order of the President, I. Lykotrafitis and K. Limniotis, IT auditors, as assistants to the rapporteur, who provided clarifications and left before the conference and decision-making, and Georgia Palaiologou, an employee of the Department of Administrative Affairs of the Authority, as secretary. The Authority took into account the following: The Authority carried out an on-site administrative audit of the national Visa Information System which is linked to the Visa Information System (hereinafter, VIS), in accordance with the provisions of Regulation (EC) no. . 767/2008 of the European Parliament and of the Council of 9 July 2008 on the visa information system and the exchange of data between Member States for short-stay visas (hereinafter, the VIS Regulation). The audit, which focused in particular on security issues of the personal data processed within the said system, was carried out on 4/4/2016 at the installation-operational site at 1-3 Kifisias Avenue, 11523 Athens, Tel.: 210 -6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -1- national system (hereinafter, ELVIS) at 1 Akadimias Street, Athens (F2 Directorate - Communications and Informatics), as well as at the facilities of the Central Service of the Ministry of Foreign Affairs (C4 Directorate) at 1 Vasilissis Sofias Street, Athens, by the Authority's auditors Ioannis Lykotrafitis and Konstantinos Limniotis (hereinafter, audit team), following the letter No. C/EX/2075 /01-04-2016 order to carry out an audit of the President of the Authority. The control was regular. In particular, the VIS system is a large information system for the exchange of data between the states located within the "Schengen area", with the aim of improving the application of the common policy in the field of visas, consular cooperation and consultation with the central visa authorities. The scope, functionality and other issues of the VIS, including personal data protection issues, are set out in the VIS Regulation, which provides for the conditions and procedures for the exchange of data between European Union (EU) countries and associated countries applying the common policy for visas. Through the VIS system, the examination of applications for short-stay visas and decisions to extend, revoke or cancel visas as well as visa controls and the verification and identification of visa applicants and holders are facilitated, so as to avoid circumventing the criteria for determining the Member State responsible for examining an application, to facilitate the fight against fraud, to facilitate controls at the external border crossing points of the Member States and on their territory, to

help identify persons who do not meet the conditions governing the entry, stay or residence in the territory of the Member States, to facilitate the application of Regulation (EC) 343/2003 (Dublin II Regulation) for the determination of the EU country responsible for the examination of an asylum application submitted by a third-country national, as well as to contribute to the prevention of threats against of internal security of the Member States. A central building block of the VIS is a central database, which was developed in accordance with Council Decision 2004/512/EC on the establishment of the Visa Information System. The following data are registered and kept in the VIS database: a) the alphanumeric data on the applicant and the requested, issued, -2- rejected, cancelled, revoked or extended visas, b) the photographs, c) the fingerprints, and d) the links to previous visa applications and to the application files of persons traveling together. Access to the VIS to enter, modify or delete data is exclusively for the duly authorized staff of the visa authorities. In terms of data retrieval, access is exclusively granted to duly authorized staff of visa authorities and authorities responsible for controls at external border crossing points, immigration and asylum controls, and such access is limited to the extent that such data are necessary for the performance of the duties of said staff. In specific cases, national authorities and Europol may request access to data entered in the VIS, for the purpose of preventing, ascertaining or investigating terrorist and criminal offences. The procedures and conditions for searching data under these circumstances, as well as personal data protection issues, are set out in Council Decision 2008/633/JHA of 23 June 2008 on access to the visa information system for authorized persons authorities of the Member States as well as Europol, to search for data for the prevention, verification and investigation of terrorist acts and other serious criminal acts (hereinafter, the VIS Decision). These data searches are conducted through central contact points in the participating countries and Europol, which check the requests and ensure legality, in accordance with the above decision. Once an application is considered acceptable in accordance with the Visa Code1, the visa authority opens the application file, entering a series of data into the VIS as specified above. After the decision to grant the visa is made, the visa authority adds other appropriate data, including the type of visa, the territory to which the visa holder is entitled to travel, the period of validity, the number of entries allowed by the visa in the territory and the duration of the authorized stay. Also, additional information must be provided if the person in charge of visas 1 Regulation (EC) no. 810/2009 of the European Parliament and of the Council of 13 July 2009 on the establishment of a Community visa code -3- authority representing another EU country to stop the examination of an application as well as when a decision is taken to refuse, cancel or revoke a visa, or extend the duration of validity of a visa. The competent visa authority may consult the VIS in order to examine applications and decisions to issue,

refuse, extend, cancel or revoke a visa, or reduce its validity. It is authorized to carry out inquiries with some of the information included in the application form and envelope. If the investigation carried out shows that the VIS contains data on the applicant, the visa authority gains access to the application file and the linked application files. For prior information retrieval, the country responsible for examining the application shall forward each information retrieval access request, with the application number, to the VIS, indicating the country or countries to be consulted. The VIS forwards the request to the country concerned which, in turn, forwards the response to the VIS which then sends the response to the requesting country. Authorities in charge of external border controls and national territories are authorized to carry out searches in the VIS based on the number of the visa sticker together with fingerprints. They may also carry out inquiries in order to verify the identity of the person and/or the authenticity of the visa and/or whether the person in question meets the conditions of entry, stay or residence in the national territories. If, based on this search, details of the visa holder are found in the VIS, the competent authorities may consult certain details of the application file. In order to identify a person who does not meet or no longer meets the required conditions, the competent authorities are authorized to carry out fingerprint searches. If the fingerprints of the person in question cannot be used or if the fingerprint search fails, the competent authorities may search the VIS with the name, sex,date and place of birth and/or with information from the travel document. These can be used in conjunction with the nationality of the person. Asylum authorities are authorized to carry out searches in the VIS based on fingerprints, but only for the purpose of determining the -4- Member State responsible for examining an asylum application, and examining the asylum application. However, if the fingerprints of the asylum seeker cannot be used or the search fails, the authorities may carry out a search based on the data mentioned above. Each application file is kept in the VIS for a maximum of five years. Only the Member State which is responsible (i.e. the one which entered the data into the VIS) has the right to modify or delete data which it has transmitted to the VIS. The VIS was gradually implemented from 2011, with the development of the system completed around the end of 2015. The VIS is connected to each country's national system through the national interface in that country. Participating countries appoint a national authority which is linked to the national interfaces and which provides access to the VIS through the competent authorities. In Greece, the responsible body for ELVIS national contact is the Ministry of Foreign Affairs. According to article 41 of the VIS Regulation, the independent national control authority of each Member State which is charged with the responsibilities referred to in article 28 of Directive 95/46/EC checks the legality of the processing of personal data carried out by the specific State -Membership to the VIS system, including the transmission of

data to and from the VIS. The national control authority ensures that, at least every four years, an audit of the data processing operations carried out in the national system is carried out, in accordance with international audit standards. Correspondingly, in article 8 of the VIS Decision, it is stated that the competent body which, according to the National Law, supervises the processing of personal data by the authorized authorities under the said Decision, checks the legality of the processing in accordance with the provisions of this Decision. This body ensures that at least every four years an audit of the processing of personal data is carried out pursuant to the aforementioned Decision and in accordance with international audit standards. For Greece, the Personal Data Protection Authority is the competent Authority provided for in Article 41 of the VIS Regulation, as well as the competent body provided for in Article 8 of the VIS Decision. This was valid both during the period of the audit in question, in accordance with the then valid Law 2472/1997 which incorporated into the national legal order Directive 95/46/EC, and after May 25, 2018, when it was put into application of -5- Regulation (EU) 2016/679 (General Data Protection Regulation - hereinafter, GDPR), which repealed Directive 95/46/EC. Based on the above, the Authority carried out an on-site administrative audit of the N-VIS national information system regarding the protection and security of personal data processed in the context of the operation of the said system, in accordance with article 19 paragraph 1 item h' Law 2472/1997 (which was in force during the audit period), with article 41 par. 2 of the VIS Regulation but also with article 8 par. 6 of the VIS Decision. In order to carry out this audit, in particular with regard to the security issues of the N.SIS II information system, the audit framework drawn up by the sub-group of IT experts of the 2nd generation Schengen Information System Supervision Coordination Group was adopted. This common framework for conducting security audits in large-scale integrated information systems was drawn up with the aim, among other things, of producing comparable results both from audits between different Member States and from audits within the same Member State but at different time periods. Since the VIS Regulation states that the national supervisory authority is responsible for conducting audits of the data processing operations carried out in the national VIS system in accordance with international audit standards, this framework was based on the international security standard ISO 27001, as the most widespread relevant standard (see also in this regard Decision no. 50/2018 of the Authority). As part of the preparation of the aforementioned administrative control in the ELVIS system, the Authority initially sent to the C4 and F2 Directorates of the Ministry of Foreign Affairs the document No. C/EX/5441/22-10-2015, with which it informed about of the upcoming audit and its purpose - that is to establish that the data processing carried out in the context of the operation of the said information system is in accordance with the provisions for the protection of personal data provided for in

the VIS Regulation, in the VIS Decision as well as in law. 2472/1997. With the same document, the Authority also sent a questionnaire specifically for the security issues of the ELVIS information system, on which - among other things - the audit was to be focused, in order to send - before the on-site audit - answers to this. Also, for each question of the questionnaire, a list of indicative proofs was mentioned to document the answer. -6- This questionnaire is part of the aforementioned common control framework. The Ministry of Foreign Affairs sent to the Authority its answers to the questionnaire in question with document number C/EIS/962/17-02-2016. Along with the document in question, the Ministry of Foreign Affairs also submitted a set of evidence, in electronic format. Subsequently, the Authority jointly determined with the Ministry of Foreign Affairs (Directorates C4 and F2) the date of the on-site audit, and the audit team carried out on April 4, 2016, based on the aforementioned audit order of the President of the Authority, an audit at the premises of the Ministry of Foreign Affairs on 1 Vasilissis Sofia St. in Athens, where the C4 Directorate is housed, and on Akademi 1, Athens, where the ELVIS information system is located and also houses the competent F2 Directorate of the Ministry of Foreign Affairs. On the part of the Ministry of Foreign Affairs, the audit was attended by Mr. Leonidas Nikolopoulos from the C4 Directorate and Messrs. Georgios Tsachtsiris and Sofia Mitrakou from the ST2 Directorate, who were given the above mandate to conduct an audit. The audit focused in particular on the organizational , technical and physical security measures applied during the processing of personal data in the context of the operation of the ELVIS system. The representatives of the Ministry of Foreign Affairs provided the control group with information both on the overall procedures followed in the context of the operation of the ELVIS system, as well as on the organizational and technological infrastructures of the system. During the on-site audit, the audit team also conducted interviews with relevant officials of the Ministry of Foreign Affairs. After the completion of the on-site audit, the Ministry of Foreign Affairs submitted to the Authority document No. C/EIS/3038/13-05-2016, with which it provided additional clarifications on issues raised by the audit team during the on-site audit audit, as well as a set of additional electronic evidences which were also requested by the audit team during the on-site audit. Subsequently, the audit team drew up the Audit Minutes (hereinafter Minutes), in which the responses/clarifications of the audited entity, as well as on-site observations of the audit team, are recorded. The Minutes were sent to the audited body by email on 10-07-2017 for -7- submission of comments and/or observations. The audited body responded with the e-mail No. C/EIS/5299/14-06-2018, while the relevant supplementary files in digital format were subsequently submitted to the Authority with the No. C/EIS /4147/10-06-2019 document, at which time the Minutes in question were also finalized (authority prot. no.: C/EIS/ C/EIS/6064/06-09-2019). The

Minutes also contain the list of Evidence attached. The control group then studied the Minutes in conjunction with the Evidence. He then drew up an Administrative Audit Conclusion (hereinafter, Conclusion), which he submitted to the Authority under no. prot. A/EIS/93/20-12-2019 document and which records, among other things, the findings regarding organizational and technical security measures, as well as recommendations for dealing with the risks created. The Authority, after consideration of the above-mentioned facts, after hearing the rapporteur and assistant rapporteurs, who then withdrew after the debate and before the conference and decision-making, and after thorough discussion, OLD IN ACCORDANCE WITH THE LAW 1.According to with article 9 of Law 4624/2019, which aims - among others -taking measures to implement the GDPR, the supervision of the implementation of the provisions of the GDPR in the Greek Territory is carried out by the Personal Data Protection Authority. 2. In article 10 par. 4 of Law 4624/2019 it is stated that in cases where independent control or supervision is provided for in European Union law or national legislation, the Authority exercises the corresponding powers and authorities. 3. According to article 94 par. 2 of the GDPR, references to the repealed Directive 95/46/EC are considered references to the GDPR. 4. In accordance with the above and taking into account what is mentioned in article 41 par. 1 of the VIS Regulation ("the authority or authorities designated by each member state and charged with the powers referred to in article 28 of Directive 95/46/ EC (…) check, independently, the legality of the processing of personal data (…) including the transmission of data to and from the VIS" but also in article 8 par. 5 of the VIS Decision ("the -8- competent body or entities that, in accordance with National Law, supervise the processing of personal data by the authorized authorities pursuant to this Decision, control the legality of the processing of personal data in accordance with this Decision", the Authority is responsible for controlling the processing of personal data , which takes place within the framework of the ELVIS system. 5. According to Article 4 of the GDPR, "personal data" means any information concerning an identified or identifiable natural person ("data subject"), while "processing" means any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, recording, organizing, structuring, storing, adapting or changing, retrieving, searching for information, using, communicating by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction. Furthermore, "controller" means 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, while when the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State.

6. In the case of data processing, in accordance with the provisions of the VIS Regulation and the VIS Decision, which is carried out through the ELVIS system, the controller is the Ministry of Foreign Affairs. 7. Regarding the security of the processing, Article 32 of the GDPR states2: "Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and seriousness for the rights and freedoms of natural persons, the controller and the processor implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks, including, among others, as appropriate: a) pseudonymization and 2 The previous legal framework (i.e. Law 2472/1997) also had a relevant provision for the requirement of processing security (as related in the conclusion of the audit in question). -9- encryption of personal data, b) the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on a continuous basis, c) the ability to restore the availability and access to personal data in a timely manner time in the event of a natural or technical event, d) a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing. When assessing the appropriate level of security, particular account shall be taken of the risks deriving from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed" . Furthermore, specifically for national visa information systems, to which ELVIS belongs, more specific security requirements are set in both the VIS Regulation and the VIS Decision. More specifically, according to article 32 of the VIS Regulation, the Member State must take the necessary measures for the relevant national VIS system, including a security plan, in order to: a) provide for the material protection of the data, as well as emergency plans for the protection of critical infrastructures; b) to prevent unauthorized persons from accessing the national facilities within which the Member State carries out actions in accordance with the purposes of the VIS (facility entry control); c) to prevent unauthorized reading; copy, modify or delete the data and their sub-subjects (sub-subject control); d) prevent unauthorized data entry and unauthorized inspection, modification or deletion of stored personal data (storage control); e) prevent unauthorized processing data in the VIS as well as any unauthorized modification or deletion of data e.g have been processed in the VIS (data input control); f) ensure that persons authorized to access the VIS only have access to data covered by their access permits, with individual and unique user identities and only with confidential -10- access codes (data access control); g) to ensure that all authorities entitled to access the VIS create profiles that describe the functions and responsibilities of persons authorized to access, insert, update, delete

and search the data and make their profiles available to the national supervisory authorities referred to in Article 41, without delay, at their request (personnel profiles); h) be able to control and ascertain to which authorities personal data can be transmitted through equipment of data transmission (control of transmission); i) to be able to control and ascertain which data have been processed in the VIS, when, by whom and for what purpose (registration control); j) to prevent unauthorized reading, copying, modification or deletion of personal data during the transmission of personal data to or from the VIS, or against the transfer of data media, mainly with appropriate encryption techniques (transfer control); k) to monitor the effectiveness of the security measures of this paragraph and to take the necessary organizational internal control measures to ensure compliance with this regulation (self-control). Furthermore, in accordance with Article 9 of Council Decision 2008/633/JHA, the Member State must take for its national VIS system the necessary measures with regard to the data to be searched by the VIS pursuant to that Decision and, in then, they will be stored, in particular: a) to provide for the physical protection of the data, as well as contingency plans for the protection of critical infrastructures; b) to prevent the entry of unauthorized persons into the national facilities where the Member State stores data (control of entering the facility); c) to prevent unauthorized reading, copying, modification or removal of data storage media (control of data storage media); -11- d) to prevent unauthorized control, as well as unauthorized modification or deletion of registered personal data (control of registration); e) to prevent unauthorized processing data from the VIS (control of data processing); f) to ensure that persons authorized to use the VIS have access only to the data covered by the authorization using an individual and exclusive code and only confidential means of access (control of access to data); g) to ensure that all authorities with a right of access to the VIS draw up lists describing the tasks and responsibilities of persons authorized to access the system and search data and that these lists are accessible to national control authorities

of article 8 paragraph 5, without delay, upon their relevant request

(personnel characteristics);

h) to ensure the possibility of being controlled and ascertained in which authorities

personal data may be transmitted with the use

data transmission equipment (control of transmission);

i) to ensure the possibility to be controlled and ascertained from

retrospectively what personal data was retrieved from the VIS, when, from

who and for what purpose (control of data entry);

j) to prevent unauthorized reading and copying of the data

during their transmission by the VIS, in particular with appropriate encryption techniques

(control of transport);

k) to check the effectiveness of the security measures set out in

this paragraph and take the necessary organizational measures

internal audit for compliance with this decision (self-audit).

8. Taking into account the above and after examining the findings that

referred to in the Audit Finding, the Authority approved the group's proposals

control.

The detailed presentation of the findings, as well as the relative risks that these

may create, are recorded – together with the corresponding recommendations for

improvement - in the attached privacy final Conclusion.

FOR THOSE REASONS

The Authority gives an order, in accordance with article 58 par. 2 d' of the GDPR, to the Ministry

of Foreign Affairs (C4 Directorate – Justice, Internal Affairs, Immigration and

Schengen, as well as F2 Directorate – Communications and IT), as responsible

processing in the sense of article 4 par. 7 of the GDPR, to comply with

recommendations mentioned in the attached final Audit Conclusion and to

inform the Authority accordingly within one year of receipt of this notice.

The president

The Secretary

Konstantinos Menudakos

Paleologo Georgia