Athens, 14-06-2018 Prot. No.: G/EX/5331/14-06-2018 HELLENIC REPUBLIC AUTHORITY FOR THE PROTECTION OF PERSONAL CHARACTER DATA A P O F A S I NO. 50/2018 The Authority for the Protection of Personal Character met in composition of the Department at its headquarters on 24/04/2018 at 10:00 a.m. upon the invitation of its President, in order to examine the case referred to in the present history. The President of the Authority, Konstantinos Menudakos, and the regular members of the Authority, Konstantinos Christodoulou, Antonios Symvonis, Spyridon Vlachopoulos, as rapporteur, Konstantinos Lambrinoudakis, also as rapporteur, Charalambos Anthopoulos and Eleni Martsoukos were present. E. Maragou, lawyer-legal auditor, and I. Lykotrafitis and K. Limniotis, IT auditors, also attended the meeting, as assistant rapporteurs, who provided clarifications and left before the conference and reception decision, and Irini Papageorgopoulou, an employee of the Authority's Administrative Affairs Department, as secretary. The Authority took into account the following: The Authority carried out an on-site administrative control in the second generation national Schengen Information System (N. SIS II) in accordance with article 19 par.1 element of Law 2472/1997, as well as article 44 par. 2 of the SIS II Regulation, regarding the protection and security of personal data that are processed in the context of the operation of the system in question. The on-site inspection was carried out on 02-03/11/2015, at the premises of the Hellenic Police Headquarters at 4 Kanellopoulou Street, P.O. 101 77, in Athens, where it is 1-3 Kifisias Ave., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@dpa.gr, www.dpa.gr -1- installed system and also houses the Departments of the Hellenic Police responsible for the system, as described below, by Filippo Mitletton, Head - during the period of the audit - of the Department of Auditors of the Authority, and the auditors of the Authority Elena Maragou, Ioannis Lykotrafitis and Konstantinos Limniotis (henceforth, audit team) following the audit order of the President of the Authority No. G/EX/5547/27-10-2015. The control was regular. In particular, the Schengen Agreement of 1985 and the Convention Implementing the Schengen Agreement (hereinafter referred to as the Schengen Agreement), which came into force in 1995, led to the abolition of internal border controls of the signatory states, as well as the creation of unified external borders, at which entry controls in the "Schengen area" are carried out on the basis of the same procedures. The same Convention established common rules for issuing visas, granting asylum and control at external borders, so that the free movement of persons within the "Schengen area" is possible without at the same time disturbing public security. The Greek Parliament ratified the Agreement and the Convention Implementing the Schengen Agreement with Law 2514/26-06-1997. The Schengen Information System (hereinafter, SIS) is a large information system, which was developed as a compensatory measure against the abolition of controls at the internal borders of the EU, and aims

to ensure a high level of security within an area freedom, security and justice, including the maintenance of public security and order and the protection of security on the territory of the Member States. Based on specific articles of the Treaty, the Member States feed the SIS with information, which falls under two categories: the first concerns wanted persons (persecuted, missing adults and minors, etc.), while the second concerns wanted vehicles or objects. Given the progress made in the field of information technologies, it was deemed necessary to develop a new system with more advanced functions, based on state-of-the-art technologies. Consequently, in Regulation (EC) no. 1987/2006 of the European Parliament and of the Council of 20 December 2006 and Decision 2007/533/JHA of the Council of 12 June 2007, laying down regulations on the establishment, operation and use -2- of the second generation Schengen Information System (henceforth, SIS II). By its decision, the competent Council of Ministers of Justice and Home Affairs of 7-3- 2013, set 9 April 2013 as the day of transition of the entire Schengen area from the original SIS system (also referred to as SIS I) to SIS II. SIS II is applied, with individual exceptions, in all EU member states, but also in the four associated member states of the European Free Trade Area: Iceland, Norway, Switzerland and Liechtenstein. SIS II focuses - like SIS I - on two major categories of information which take the form of alerts concerning, firstly, persons - who are wanted, who have disappeared, who are wanted for assistance in judicial proceedings, for discreet or specific checks, or are third-country nationals who are subject to a ban on entry or residence in the Schengen area, and, secondly, with objects - such as vehicles, travel documents, credit cards, for seizure or use as evidence in legal proceedings, or for discretionary or specific checks . Depending on the type of alert, SIS II is governed by either Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System for registration procedures falling under Title IV of the Treaty establishing the European Community - former first pillar - (hereinafter referred to as the "SIS II Regulation") or by Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) as regards the procedures fall under Title VI of the Treaty establishing the European Community - former third pillar - (hereinafter referred to as the "SIS II Decision"). Furthermore, SIS II is also governed by Regulation (EC) 1986/2006 of the European Parliament and of the Council on access to it by Member State authorities responsible for issuing vehicle registrations, which replaced Article 102A of Schengen Agreement. The main changes brought about by SIS II concern the technical capabilities of the system, better data searchability (increased search criteria) and provision of more information in the system's data. When the alert in SIS II concerns a person, the name, surname and any aliases, gender, details of the

decision based on which the alert is entered and the tactics followed must always be included. The registration may also include, if available, information such as particular, objective and unalterable physical characteristics, place and date of birth, photographs, fingerprints, nationality or nationalities, indication that the person in question carries a weapon, is violent or has escape, the reason for the alert, the authority entering the alert, links to other alerts entered into SIS II pursuant to Article 37 of the SIS II Regulation or Article 52 of the SIS II Decision. SIS II consists of a central system (hereafter 'central SIS II'), a national system (hereafter 'N.SIS II') in each Member State, which communicates with Central SIS II, and a communication infrastructure between the central system and the national systems providing an encrypted virtual network used only for SIS II data and the exchange of data between the authorities responsible for the exchange of all supplementary information. Each Member State is responsible for the establishment, operation and maintenance of its national system and for its connection to the central system and designates an authority, the national SIS II service (N.SIS II service), which has the central responsibility for the national SIS II project. This authority is responsible for the smooth operation and security of its national system. Furthermore, each member state of the Schengen area must set up a central authority, which will act as a single point of contact and coordination for the exchange of additional information about data registered in the system. This point of contact is called the "SIRENE Department" (Supplementary Information REquest at the National Entries). At the national level, the responsibility for the orderly operation of N.SIS II (installation, technical support, performance monitoring and ensuring smooth operation) rests with the Operations Department of the IT Directorate of the Hellenic Police Headquarters (see art. 22 par. 4 of Presidential Decree 178/2014 regarding the organization of the Greek Police Services).Also,the 3rd SIRENE Department of the Directorate of International Police Cooperation of the Hellenic Police Headquarters is responsible for managing the information registered in SIS II (in accordance with art. 8 par. 4 of Presidential Decree 178/2014), as provided in nos. 7 par. 2 of the SIS II Decision and the SIS II Regulation regarding the exchange of additional information related to the data -4- registered in SIS II. As a guarantee of the citizens' rights, the SESA contains a special chapter on the protection of personal data and their security in the context of the operation of the Schengen Information System (Articles 102 – 118). In particular, the SESA provides, among other things, for the operation of an independent Control Authority in each contracting state, which is competent to exercise independent control of the file of the national section of the Schengen Information System and to check whether the processing and use of those registered in the system information Schengen data violate the rights of the persons concerned (Article 114 TEC). Accordingly, both the SIS II Regulation and the SIS II Decision also contain a special

Chapter for the protection of personal data. This chapter provides that an independent authority in each Member State will exercise independent control as to the legality of the processing of SIS II personal data in the territory of the Member State to which they belong and their transmission from that territory, as well as the exchange and further processing of supplementary information. In particular, it is stipulated that the national supervisory authority ensures that at least every four years an audit of the data processing operations carried out in N.SIS II is carried out in accordance with international audit standards. In Greece, the relevant supervisory authority has been assigned by article 19 par. 1 item. n' of Law 2472/1997 to the Authority. In the context of this competence, the Authority carried out the above-mentioned on-site administrative control of the second generation national Schengen Information System (N. SIS II) regarding the protection and security of the personal data that exist and are processed in the context of the operation of the system in question. In order to carry out this audit, in particular with regard to the security issues of the N.SIS II information system, the framework for conducting audits prepared by the sub-group of IT experts of the Supervision Coordination Group of the Schengen Information System 2nd generation (in which participating, from the Greek Authority, I. Lykotrafitis, IT auditor). This common framework for conducting security checks in large-scale integrated information systems, such as SIS II, was drawn up with the aim, among other things, of producing comparable results both from checks between different Member States and from checks from the same Member State but in -5- different time periods. Given that in the SIS II Regulation (art. 44, par. 2) it is stated that the national supervisory authority is responsible for conducting audits of the data processing operations carried out in N.SIS II in accordance with international audit standards, this framework was based on the international security standards ISO 27001 and 27002, as the most widespread relevant standards. In the context of the preparation of the aforementioned administrative control in the national N.SIS II, the Authority initially sent to the SIRENE Department of the Directorate of International Police Cooperation of the Hellenic Police the letter No. C/Eξ/4155-2/09- 10-2015 document, with which he informed about the upcoming audit and its purpose - namely to establish that the data processing carried out in N.SIS II is in accordance with the provisions for the protection of personal data provided for in the SIS II Regulation, in SIS II Decision, as well as in Law 2472/1997. With the same document, the Authority also sent a questionnaire specifically on the security issues of the N.SIS II 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. This questionnaire is part of the aforementioned common control framework. The Hellenic Police sent the Authority its answers to the

aforementioned questionnaire with the Authority's No. A/EIS/133/29-10-2015 document. Subsequently, the Authority informed the SIRENE Department of the Directorate of International Police Cooperation of the Hellenic Police, with document No. C/Eξ/5548/27-10-2015, about the dates on which the on-site inspection would be carried out . Following this, in accordance with the above-mentioned inspection order of the President of the Authority, the inspection team carried out an inspection on November 2 and 3, 2015 at the premises of the Hellenic Police at the address Kanellopoulou 4, P.O. 101 77, Athens, where the N.SIS II information system is located and also houses the competent Services of the Hellenic Police. On the part of the Greek Police, Mr. A, Head of the Department, from the SIRENE Office of the Directorate of International Police Cooperation, and Mrs. C, Head of Department B, from the Informatics Directorate, attended the inspection. of Information Security and Personal Data, D, -6- Head of the Office of Information Security and Risk Analysis, E, Head of Technical Support N.SIS II of the Operational Operation Department, and F, an employee of the Information and Personal Data Security Department, and from Directorate of Foreigners, Mr. Z, Director. The audit focused on: a) compliance with the basic principles of data processing, i.e. principle of purpose, proportionality and time of data retention as well as the manner and process of exercising the rights of subjects, and b) organizational, technical and physical measures security measures applied during the processing of personal data in the context of the operation of the N.SIS II system. The above audit order was delivered to the representatives of the Hellenic Police, who provided the audit team with information both on the overall procedures followed in the context of the operation of the N.SIS II system, as well as on the organizational and technological infrastructure of the system. During the on-site audit, the audit team simultaneously conducted interviews with competent employees of the Hellenic Police Department of the International Police Cooperation Directorate (SIRENE Department), the IT Department (Operational Operation Department and Information Security and Personal Data Protection Department) and the Aliens Department. The responsibilities of the said Departments and the Directorate, in relation to N.SIS II, are the following: a) The SIRENE Department exchanges information with the National SIRENE Bureaus of the other contracting parties of the SESS, conducts consultations with the contracting parties, where this is required, for the registration or non-complementary data or the deletion of data in the N.SIS, in the context of the implementation of the SESS, it ensures the cooperation with the other national Services and the international bodies, to whose competence the handling of the mentioned issues falls in SESS et al. (see art. 8 par. 4 of Presidential Decree 178/2014 regarding the organization of the Greek Police Services). b) The Operational Operation Department includes the so-called SIS Office, which is responsible for the installation, technical support,

performance monitoring and ensuring the smooth operation of N.SIS II, including its interconnections with information systems of third parties, as well as the observance of the corresponding database (see art. 22 par. 4 of PD 178/2014 regarding -7- the organization of the Hellenic Police Services). c) The Department of Information Security and Personal Data Protection is responsible for overall information security issues of the systems and infrastructures of the Hellenic Police, such as the drafting, review and updating of the Information and Information Systems Security Policy, the monitoring and opinion on incidents related to information security and the protection of personal data, etc. (see art. 22 par. 5 of Presidential Decree 178/2014 regarding the organization of the Hellenic Police Services). d) The Directorate of Aliens is responsible for the registration or deletion as the case may be in the lists of undesirables (see article 12 of Presidential Decree 178/2014 regarding the organization of the Hellenic Police Services). This competence is further specified in article 2 of the joint ministerial decision No. 4000/4/32-la' of 5.10.2012 on the criteria and procedure for the registration and deletion of foreigners in the National List of Undesirable Foreigners, as amended byjoint ministerial decision No. 4000/4/32-n from 31.3.2017 in order to harmonize its provisions with those of Law 4055/2012 and Law 4322/2015. At the same time, the Directorate of Aliens has the authority for registrations with the aim of prohibiting the entry or residence of third country nationals according to art. 24 of Regulation 1987/2006, which are carried out by decision of the Director of the Aliens Directorate, as long as there is a registration in the National List of Unwanted Aliens. In particular, the Directorate of Foreigners of the Headquarters of the Hellenic Republic of Greece. is responsible for the registrations carried out through information and data, which are supplied by the Greek embassies and consulates in the event that there are reasons of public order and security, related to indications of the commission of a serious criminal act abroad, while for all other registrations the competence belongs to the Directorate of Aliens of Attica, to the regional offices of Aliens and to the Directorate of State Security of EL.AS. Also, as part of the audit, regarding the security issues of the N.SIS II information system, the audit team requested a series of electronic proofs (hereinafter Proofs). The evidence was electronic, compiled and delivered by the Information Security and Privacy Department during the audit as a compressed electronic file. The proofs in question were submitted to the Authority with document No. G/EIS/5776/06-11-2015: to -8- ensure the integrity of the electronic proofs, a cryptographic hash function was applied using appropriate software. Subsequently, the protocol of receipt of the evidence was sent, with the document No. C/EX/5866/11-11-2015, to the aforementioned Department. Subsequently, the audit team drew up the Audit Minutes (hereinafter Minutes) regarding the security part of the N.SIS II information system, 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 with the Authority's document No. A/EX/29/09-03-2016 to the audited body for submission of comments and/or observations. The controlled entity responded with the no. 1795/16/609085 and from 29-03-2016 document (Authority's order no.: A/EIS/38/01-04-2016), while subsequently new clarifications were requested from the Authority with order no. C/EX/2511/19-04-2016 document, which were provided with the no. 1795/16/800627 and from 23-04-2016 a document of the Informatics Department of the Hellenic Police (authority no.: C/EIS/2798/28-04-2016), when the aforementioned Minutes – taking into account the comments of the audited body – finalized with the document No. Prot. C/EIS/4830/29-07-2016). The Minutes also contain the list of Evidence attached. The review team 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/20/06-03-2018 document and which records, among other things, the findings regarding security measures or personal data protection procedures identified, as well as recommendations for dealing with the risks created. The Authority, after examining the aforementioned data, after hearing the rapporteur and the assistant rapporteurs, who then left, and after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. Article 2 of Law 2472/1997 states that "personnel data character" is "any information that refers to the data subject". "Data subject" is "the natural person to whom the data refers, and whose -9- identity is known or can be ascertained, i.e. can be identified immediately or indirectly, in particular on the basis of an identification number or on the basis of one or more specific elements that characterize his condition in terms of physical, biological, mental, economic, cultural, political or social". In the same article, personal data processing is defined as "any task or series of tasks carried out by the State or by a legal entity under public or private law or an association of persons or a natural person with or without the aid of automated methods and applied to personal data, such as collecting, recording, organizing, maintaining or storing, modifying, exporting, using, transmitting, disseminating or otherwise making available, associating or combining, linking, binding (locking); deletion, destruction" and as controller "anyone who determines the purpose and manner of processing personal data, such as a natural or legal person, public authority or agency or any other organization", while as processor is defined as "anyone who processes data of a personal nature on behalf of a controller, such as a natural or legal person, public authority or agency or anyone else organization". 2. Article 4 of Law 2472/1997 provides that "In order for personal data to be lawfully processed, it must: a) Be collected in a lawful and lawful manner for specified, clear and lawful purposes and undergo lawful and lawful processing in view of the these purposes. b) To be relevant, convenient, and no more than is required each

time in view of the purposes of the processing. c) To be accurate and, if necessary, to be updated. d) To be kept in a form that allows the identification of their subjects only during the period required, at the discretion of the Authority, for the realization of the purposes of their collection and their processing." Especially regarding the time of observance, it is noted that, according to the articles 29 of the SIS II Regulation and art. 44 of the SIS II Decision, the expediency of keeping the alerts is reviewed within three years, while for alerts concerning persons for the purpose of discretionary monitoring or special control, said review takes place within one year. -10- 3. According to the articles 12 and 13 of Law 2472/1997 the data subject has the right to access the data concerning him and the right to object to the processing concerning him, respectively. These same rights are also included in art. 41 of Regulation 1987/2006 SIS II and in art. 58 of Decision 2007/533 SIS II. Specifically, based on the above, the data subject has the right, on the one hand, to request and receive from the controller access to the data concerning him and registered in SIS II and, on the other hand, to request the correction or deletion of data, as a more specific form of right of objection, concerning it and containing a factual or legal error. The controller is obliged to respond within fifteen (15) days. 4. Article 10 of Law 2472/1997 states that: "1. The processing of personal data is confidential. It is carried out exclusively and only by persons who are under the control of the data controller or the data processor and only on his instructions. 2. To carry out the processing, the controller must select persons with corresponding professional qualifications who provide sufficient guarantees in terms of technical knowledge and personal integrity for the observance of confidentiality. 3. The controller must take the appropriate organizational and technical measures for the security of the data and their protection against accidental or unlawful destruction, accidental loss, alteration, prohibited dissemination or access and any other form of unlawful processing. These measures must ensure a level of security commensurate with the risks involved in the processing and the nature of the data being processed. Without prejudice to other provisions, the Authority provides instructions or issues regulatory acts in accordance with article 19 par. 1 j' to regulate issues related to the degree of security of data and computing and communication infrastructures, the security measures that are necessary to be taken for each category and data processing, as well as for the use of privacy-enhancing technologies. 4. If the processing is carried out on behalf of the person in charge by a person not dependent on him, the relevant assignment must be made in writing. The delegation obligatorily stipulates that the person performing the processing only carries out it at the behest of the person in charge and that the other obligations of this article fall accordingly on him as well". -11- Also, according to no. 10 of the SIS II Regulation, but also with art. 10 of the SIS II Decision, the Member State must take the necessary measures for the relevant

N.SIS II, which include a security plan, so that: a) the physical protection of the data is foreseen, as well as emergency plans need to protect critical infrastructure,

b) to prohibit unauthorized persons from entering the premises where the processing of data and in particular personnel data is carried out character (control of entry to premises),

c) to prevent unauthorized reading, copying, modification or removal of data storage media (control of storage media data),

d) to prevent the unauthorized entry of data and the non authorized inspection, as well as unauthorized modification or deletion of registered personal data (registration check in a file),

e) prevent the use of automatic data processing systems by unauthorized persons using data transmission equipment (usage control),

f) to ensure that the persons who are authorized for the using an automatic data processing system have access only the data covered by the authorization provided and that only individual and exclusive access is used for this access password and confidential access method (control of data access),

g) to ensure that all authorities with a right of access to SIS II or to data processing facilities, prepare statements with the duties and responsibilities of the persons authorized to have access to the system, enter it, update, delete and to investigate the data, and that the aforementioned situations are accessible to national supervisory authorities without delay, upon their relevant request

(personnel characteristics),

h) to ensure the possibility to control and ascertain which

authorities personal data may be transmitted with the use

data transmission equipment (transmission control),

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

retrospectively what personal data was entered into the automated system

data processing, when, by whom and for what purpose (control of input),

j) to prevent, in particular by using appropriate encryption techniques, the non-

authorized reading, copying, modification or deletion of the data, v

the transmission of personal data and during the transfer of the media

their storage (transport control),

k) check the effectiveness of security measures and take them

the necessary organizational internal control measures to carry out internal

controls in order to comply with the provisions of this regulation

(self-check).

Furthermore, according to nos. 11-14 of the SIS II Regulation, but also respectively

with the nos. 11-14 of the SIS II Decision, the Member State, among other things, must:

a) to apply the applicable rules on professional secrecy or

equivalent obligation of confidentiality for all persons and all bodies that

deal with SIS II data and supplementary information

b) ensure that a record is kept of each and every access

and any exchange of personal data carried out on

frameworks of the central SIS, in order to check the legality of the search,

as well as the legality of data processing and to ensure the

self-control and the proper functioning of N. SIS II, as well as the integrity and

data security.

c) ensure that any authority that has a right of access to his data

SIS II to take the necessary measures to comply with the SIS II Regulation

and the SIS II Decision and to cooperate, if necessary, with the national

supervising Authority.

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

referred to in the Conclusion, the Authority approved the audit team's recommendations.

The detailed presentation of the findings, as well as the risks they may pose

to create, are recorded in the attached confidential final Conclusion.

FOR THOSE REASONS

-13-

The Data Protection Authority issues a warning to Hellenic Headquarters

Police (Directorate for International Police Cooperation – SIRENE Department, as well as

IT Department), as data controller within the meaning of art. 2 pcs. g'

of Law 2472/1997, to comply with the recommendations referred to in the attached

final Finding of the audit and to inform the Authority accordingly within one year from

download the Finding.

The president

The Secretary

Konstantinos Menudakos

Irini Papageorgopoulou

-14-