COUNCIL OF THE EUROPEAN UNION

Brussels, 19 May 2010

10608/1/09 REV 1

LIMITE

SCH-EVAL 82
COMIX 473

DECLASSIFICATION

of document:	ST 10608/09 RESTREINT UE
dated:	4 June 2009
new classification:	LIMITE
Subject:	Schengen evaluation of ROMANIA - Draft Report on Data Protection (April 2009)

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (07.08.2020)

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

COUNCIL OF
THE EUROPEAN UNION

Brussels, 4 June 2009

10608/09

RESTREINT UE

SCH-EVAL 82
COMIX 473

REPORT

From :	Schengen Evaluation Committee
To :	Schengen Evaluation Working Party
Subject :	Schengen evaluation of ROMANIA - Draft Report on Data Protection (April 2009)

The current report is based on the replies of **Romania** to the questionnaire and includes the results of the visit, following the evaluation and the drafting session of the Evaluation Committee during the visit. The comments of the Romanian authorities are set out in the body of the text.

TABLE OF CONTENTS

*

*   *

REPORT ON DATA PROTECTION

This report was drafted by the Evaluation Committee and is brought to the attention of the Sch-Eval Working Party for discussion and subsequent submission to the Council.

1. Introduction

Based on the mandate of the Schengen Evaluation Group (SCH/Com-ex (98) 26 def), the Schengen Evaluation Programme 2008-2013 (doc. 6949/3/08 REV3), the Provisional list and indicative calendar of evaluations for 2009 (doc.11602/1/08 REV 1) and the Overview of programmes, participants, technical details for the Schengen evaluations in 2009 (doc. 5160/1/09 REV 1), experts carried out a Schengen evaluation of **Romania** in the field of data protection.

The following experts participated:

DELETED

The evaluation took place in Bucharest on 29 and 30 April when the presentation of the national representatives of Romania was given and the questions of the experts discussed.

2. Management summary

The Committee was very impressed by and pleased with the quality of the documents provided, the preparation, organization and the excellent and clear presentations provided by the authorities involved.

3. Legislation

The Romanian legislation related to the protection of personal data is the following:

- Law no. 682/2001 on ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981 [1]
- The Romanian Constitution- article 26
- Law no. 55/2005 on ratifying the Additional Protocol to the Convention for the Protection of Individuals regarding Supervisory Authorities and Transborder Data Flows, adopted in Strasbourg, 18 November 2001, CETS No. 181 [2]
- Law no. 677/2001 on the protection of individuals with regard to personal data processing and the free movement of such data[3] implementing the provisions of Directive 95/46/EC (annex 1). The Romanian law, within the stated limits, also applies to the processing and transfers of personal data, carried out in the context of crime prevention, criminal investigation and repressing activities and maintaining public order, and also to other activities performed in the domain of criminal law, within the limits and restrictions stated by the law (Article 2 paragraph (5)). Also, this law ensures a level of protection for personal data which is aligned to the requirements laid down in Article 117 and Article 126 of the Schengen Convention
- Law no. 102/2005 which provides the setting up of National Supervisory Authority for Personal Data Processing as a public, autonomous and independent authority from any other public body, as well as from any natural or legal person from the private area, which fulfils the requirements of art. 114 of the Schengen Convention [4] (annex 2).
- GEO no. 128/2005 on the setting up, organizing and functioning of the National Information System of Alerts, approved and modified by Law no. 345/2005 [5] (annex 3). According to article 1 paragraph (3) of GEO no. 128/2005, NISA will provide data to SIS, in line with the European regulations in the field, once Romania will join Schengen area.
- GD no.1411/2006 for approving the methodological norms of GEO no.128/2005 [6] (annex 4).

During 2009, the current national legislation on NISA will be updated in order to ensure the compatibility with SIS II legislation (new categories of data, functionalities, access rights, etc.). Currently, the national legislation in force on NISA is under revision.

At present, at the suggestion of the National Supervisory Authority for Personal Data Processing (NSAPDP), Recommendation (87) 15 is in the process of being implemented, by the competent authority, through a normative act with a superior legal force.

---

1 OJ no. 830/21 December 2001.
2 OJ no 244/23 March 2005.
3 OJ no. 790/12 December 2001.
4 OJ no. 391/9 May 2005.
5 OJ no. 1086/2 December 2005.
6 OJ no. 856/19 October 2006.

The general rules as far as data protection is concerned are stipulated in Law no. 677/2001, as amended. Specific provisions on NISA can be found in GEO no. 128/2005 and also in GD no. 1411/2006.

NISA will provide data to SIS, in line with the European regulations in the field, once Romania will join the Schengen area.

Based on the EU Accession Treaty, all provisions on personal data protection in relation to SIS are binding for Romania. Data protection rules as regards the protection of SIS data will be:

- Only the competent authority issuing the alert shall be authorized to modify, add, correct or delete data, which it has entered, until the expiry period established by law.
- Competent authorities consult only alerts contained in N.SIS, only the authorized users are granted access.
- Alerts contained in N.SIS cannot be transferred, unloaded or copied. Each supply and/or access of data with personal character shall be logged in NISA in order to verify the admissibility of introduction and/or search. The record from the log files can be used only in this purpose and shall be erased the soonest after a period of one year and the latest after a period of three years.
- With purpose of supply and/or access of alerts contained in N.SIS, the competent authorities shall issue a common methodology including technical, operative and procedure measures, correlated with security requests issued by national competent authorities. This methodology is planned to be ready at the beginning of 2010, before NISA is operational.

Comments and recommendations of the Evaluation Committee

The Constitution provides for the protection of privacy, but not specifically for the protection of personal data. The legal framework required to fully implement the Schengen *acquis* is largely in place and is expected to be completed by the end of this year with the adoption of two relevant laws regulating processing of personal data related to the Schengen Information System (in May and September respectively). For instance, the draft Law regarding the regulation of the personal data processing implementing recommendation R (87)15 passed successfully in the higher Chamber but is still to be adopted by the lower Chamber. This Law should provide for the provision of adequate security measures.

Comments of Romania

The draft Law regarding the regulation of the personal data processing implementing recommendation R (87)15 was adopted by the lower Chamber of the Romanian Parliament on the 19th of May 2009. It will be sent for promulgation to the Romanian President and afterwards it will be published in the Official Journal.

The Law will be implemented through The Instructions of the ministry of administration and interior on the organizational and technical measures for providing the security of the personal data processing carried out by the data controllers of the MAI.

The instructions represent working procedures addressed and applicable to data controllers who process personal data within the Ministry of Administration and Interior.

The Instructions describe the organizational and technical measures that should be fulfilled by any controller which process personal data within MAI, in order to ensure an adequate protection of personal data.

The draft Instructions are pending endorsement by the NSAPDP.

The Committee will be kept informed of any new developments in this field

4. Data Protection Authority: structure, powers, budget and supervisory rule

Organization and structure

According to the provisions of Law no. 677/2001 and Law no. 102/2005, the National Supervisory Authority for Personal Data Processing (NSAPDP) is the only competent authority to supervise and control the legality of the personal data processing.

The NSAPDP is a public authority, autonomous and independent from any other public body, as well as from any natural or legal person from the private area, which exercises its competences established by the legal provisions in the data protection field and the free movement of such data.

The procedure of appointing the NSAPDP‘s president provides that he/she is appointed by the Romanian Senate.

The NSAPDP’s independence is also ensured through the way it is financed, having its own budget, which is part of the state budget.

Specifically, based on the provisions of GEO no. 128/2005, the management and the use of data contained in NISA, on the processing of personal data, are subject to the control of the NSAPDP.

The NSAPDP’s concrete powers are stipulated in the general provisions of Law no. 677/2001 and Law no. 102/2005. As regards NISA data, the specific provisions are to be found in GEO no. 128/2005, which provide that the management and use of data contained in NISA, regarding the processing of personal data are subject to the control of the NSAPDP. Law no. 102/2005 provides that the NSAPDP has the right to carry out inspections ex-officio or upon request.

While exercising its investigative powers, in case the NSAPDP notices inconsistencies with the provisions of the law, it may apply sanctions, the legal maximum limit for a fine being up to 50.000 RON (approximately 13.000 EUR). By decision, it may also dispose the temporary suspension or cessation of the personal data processing, the partial or total erasure of the processed data. In case it presumes that the data controller has committed a criminal offence, the NSAPDP may also notify the criminal law enforcement authorities. In order to defend the data subject’s rights safeguarded by the law, the NSAPDP has the right to address to the court of law.

The state and professional secrecy cannot be invoked in order to prevent the exercise of the powers of NSAPDP as these are set out by law. When protection of the state or professional secrecy is invoked, the NSAPDP has the obligation to keep the secret. The entire staff of the NSAPDP has the obligation of professional secrecy, except for the cases set out by law, regarding the confidential or classified information they have access to, while carrying out their duties in exercising their powers, even after having ceased their employment legal relations with the NSAPDP.

While exercising its supervision powers, the NSAPDP can also make recommendations and binding instructions in order to improve the activity of the data controllers.

Supervision

The NSAPDP will not have direct, automatic access to the data stored in the N.SIS II. According to the general national legislation, in order to carry out an inspection, the NSAPDP may request any documents it considers necessary, including those related to the data processed within NISA.

During the inspections, the data controllers are obliged to supply the NSAPDP with any information related to data processed and any documents or records regarding the personal data processing.

If necessary, with respect to the nature of the investigation, NSAPDP may organize supervision in parallel. Upon Schengen accession, NSAPDP will envisage the performance of periodical inspections concerning article 96 and article 99 alerts. Considering the Pilot Phase for NISA, the NSAPDP envisages an inspection before the introduction of SIS II.

According to the provisions of Law no. 102/2005, the staff scheme of the NSAPDP was established at 50 positions (current figure). In the Budget Proposal for 2009, the NSAPDP has included the necessary funds in order to cover the financial and technical requirements imposed by the implementation of data protection guarantees in accordance with the Schengen Convention. At present, there is a proposal of a normative act amending Law no. 102/2005 on setting up, organizing and functioning of the National Supervisory Authority for Personal Data Processing, with a view to increase the number of positions included.

The NSAPDP will organize, with the help of TAIEX, an expert mission on “Strengthening the supervisory authority’s attributions of control in the field of Schengen”, which targets the (present and future) staff of the supervisory authority with competences related to Schengen, including supervision of the SIS.

Comments and recommendations of the Evaluation Committee

The NSAPDP acts independently. There is also evidence of a high level standard in the implementation of personal data protection as defined by national legislation and good cooperation between the NSAPDP and other public bodies involved in data protection; the Committee welcomed in particular the participation of the NSAPDP in the training of the police.

The Committee underlines the need to provide the above mentioned authority with adequate premises given the fact that its tasks have been expanded inter alia through the rising number of complaints by data subjects (ten times in the last year only), and further growth should be expected following the accession of Romania to the Schengen area. The Committee doubts whether the resources currently allocated to the investigative department are sufficient given the number of investigations they perform on a yearly basis and taking into account quality requirements.

In general, the Committee was satisfied with inspections in the authorities which will use the Schengen Information System (i.e. the Ministry of the Administration and Interior, the Police Units and the Consular Posts) conducted by the NSAPDP since 2006. The Committee took note of the overall number of inspections and the fact that all the data bases maintained by the Ministry of Administration and Interior have been subject to an inspection. The findings and imposed corrective measures seem to have lead to the improvement of the processing and use of personal data. The Committee would welcome an overview of response or follow-up to inspections conducted in the above authorities. It is evident that NSAPDP´s supervisory role is accepted; this has been confirmed and reinforced by the rulings of the court in cases the inspected authority appealed the Commission's decisions. The NSAPDP has the capacity to act independently and it can have its decisions enforced effectively.

Comments of Romania
Romania will keep the Committee informed.

5. Rules of access for individuals/Rights of data subjects

According to Law no. 677/2001 correlated with GEO no. 128/2005, data subjects have direct access to the data stored in NISA.

Regarding the data contained in NISA, any interested person can make a request to the MAI for information regarding his/her personal data in NISA. Under the law, any prejudiced person can request legal redress of the prejudice caused by introducing or exploiting his/her personal data in NISA.

The NSAPDP could examine the data contained by an alert, ex-officio (periodical investigations) or based on a complaint, with regard to the observance of the data protection rules.

In case of exercising the right of direct access by the data subject, the legal time limits for the competent authorities to comply with, are in line with the general provisions in the data protection field (within 15 days from receiving the request). If the competent authorities do not comply with the legal time limits, the data subject has two options: to file a complaint to the NSAPDP or to address the matter directly to the court of law.

The data subject has a direct access right.

In defense of the rights set out by the present law, the data subject may file a complaint to the NSAPDP but only after he/she addressed previously the data controller.

Except for the cases in which a delay would cause imminent and irreparable damage, the petition submitted to the NSAPDP must not be addressed earlier than 15 days since filing in a complaint on that same case to the data controller.

If the complaint is solid (well-founded), the NSAPDP may issue a decision disposing the temporary suspension or cessation of the personal data processing or partial or total erasure of the processed data. The motivated decision will be communicated to the interested parties within no longer than 30 days notice from the registration of the complaint. Within 15 days of communication, the data controller or the data subject may submit an appeal to the competent administrative court of law, under the sanction of decay. The court's decision is permanent and irrevocable. The complaint addressed to the court of law is exempted from stamp tax.

At the same time, in order to protect the rights of the data subjects, guaranteed by Law no. 677/2001, as amended, the NSAPDP may apply sanctions or address to the court of justice. In these latter cases, procedures may take longer.

The right in Law no. 544/2001 concerning the free access to public information, as amended, provides each person access to public information and has to be interpreted in relation with the general data protection rules which establish certain exceptions (e.g. information related to personal data is exempted from public access).

Comments and recommendations of the Evaluation Committee

With regard to the right of direct access, the Committee found the obligation of public authorities to keep records of the execution of rights and to inform the NSAPDP on a yearly basis on the cases in which access has been refused, relevant.

The Committee welcomes the fact that the right of access and the right of rectification and deletion are in compliance both with national and international legislation even in cases where the data subject is not granted the access. The Committee took note of the fact that the data subject can request access (free of costs) at least once a year; further clarification is needed on how future requests in respect to executing data protection rights in the Schengen Information System will be payable in such a way that it will not impede data subjects to execute these rights from abroad. The Committee considers positive that both the Police and the other Departments involved in the processing of personal data have appointed a person responsible for personal data protection, in addition to the Department within the MAI. An entire and comprehensive system of staff training which includes E-learning (AEL) inter alia on Schengen is maintained.

Comments of Romania

In case a data subject makes use of his/her right more than once a year, NSAPDP recommends that, if a tax will be eventually established, it will not be prohibitive so as not to restrain the right of access to the personal data.

6. Rules for logs/IT-security

The access and the use of data contained in NISA will be carried out according to the law, by the competent authorities and only for the purpose of fulfillment of attributions established by law and according to the conditions provided therein. The data are being used only for the purposes for which they have been introduced in NISA. The specific rules concerning the processing of SIS data in the national system and storage of the data are stipulated in GEO no. 128/2005 and its methodological norms.

According to general provisions on data protection, data must be stored in such a manner which allows the identification of the data subjects exclusively for the period of time necessary to achieve the purpose for which the data are collected and further processed.

The competent authorities are responsible for the accuracy, level of emergency, up to date character and legality of data introduced in the NISA. Only the competent authority issuing the alert shall be authorized, until the expiry period established by law, to modify, add, correct or delete introduced data.

The competent authorities consult only the alerts contained in NISA which are necessary for the fulfillment of their attributions and they ensure that only authorized personnel has access to data. The personal data introduced in NISA are being stored only for the period necessary for achieving the purpose for which they have been entered. The archive will be kept as long as needed. Final paper files will be kept one year and will be destroyed after this period.

According to data protection rules, the data controller has the obligation to apply adequate technical and organizational measures in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective transmission of data is done within a network, as against any other form of illegal processing. Specifically, the data controller and the competent authorities are obliged to prevent the loss of the information and to ensure their recovery in case of natural disasters.

Thus, there will be a SIS II national copy only with read access for end-users. Romania does not plan to duplicate SIS data. The authorities are planning to implement a Disaster Recovery solution for SIS in another location than Bucharest that will be established at the beginning of this project. The Disaster Recovery solution is going to contain off-line identical copies of the data bases of N.SIS including SIS II.

According to the provisions of GEO no. 128/2005, the data controller and the competent authorities have the obligation to adopt security measures concerning the use and management of NISA which refer to the control of the access to equipments in order to avoid the access of unauthorized persons. The users' access using fixed stations will be certified and authorized based on digital certificates (Public Key Infrastructure – PKI).

The mobile terminals will communicate with NISA using the TETRA Network. This network enforces a limitation of the bandwidth for this kind of terminals. Thus, the certification and authorization of the users using mobile terminals will not be realized by digital certificates, but will be based on the equipment identification number, user name and password. A policy that will include the obligation to change regularly the access password will be established and implemented.

In order to ensure the users' access to NISA using TETRA terminals, a transcoder device will be ensured at the entrance point to NISA, having the role to ensure the protocol conversion from WAP to HTTP.

Only authorized users will be allowed access to SIS data. Each end user will be classified into groups with predetermined rights of access (roles) necessary for the user to perform his/her duty. The access control to N.SIS will allow the possibility to restrict the access to services and data, based on the roles assigned to the users. Every access will be logged and evaluated according to the requirement of the supervisory authority.

As to the protection of SIS data, the data controller and competent authorities will take technical, operational and procedural measures according to the following principles: confidentiality, integrity, availability, identification, authentication and authorization.

During the N.SIS implementing phase, a Security Plan will be drafted which will cover all the aspects related to organizational security, intrusion detection and protection against viruses. Security measures deriving from this plan, internal regulations and methodology for the use of the IT system and the terms stipulated in the Schengen Catalogue of Best Practices and Recommendations for SIS/SIRENE will apply to all the locations and users within MAI where SIS data will be accessed in order to ensure the adequate security level.

Outside of MAI, other locations and users where SIS data will be accessed will apply security measures in accordance with the Schengen Catalogue of Best Practices and Recommendations for SIS/SIRENE.

Staff dedicated to implementing, ensuring and monitoring all the security aspects for the system, will be designated. The service staff and SIS data users will be obliged to secure the workplace where SIS data are accessed and handled, against abuse after they leave the workplace.

The main and backup N.SIS workplace will be situated in the building of SIS National Centre which will be guarded. Access within will be secured by a monitoring video surveillance system and an electronic entrance control, which will also ensure restricted access to individual rooms. The access in different rooms within this Centre will be granted individually and differently for staff working in this location in order to fulfill the necessary tasks established under the job description. All accesses will be saved and the logs will be kept as long as necessary.

The users' access using fixed workstations will be granted and authorized based on a digital certificate. The communication established for accessing SIS data for fixed workstations will be realized through MAI's internal secured network. Also, application security mechanics (for example HTTPS protocols) will be used for sessions opened for accessing SIS data. MAI's internal Public Key Infrastructure will provide digital certificates for the SIS users.

All SIS users will have to use a smartcard or token which can not be used without a password and cannot be transmitted to another SIS user. The user using mobile terminals for accessing SIS data will be authorized based on user name and password and the access to data will be possible only for certain mobile terminals based on the equipment identification number. The communication established for mobile access will be secured based on the security measures implemented on TETRA Network and established through TETRA Standard. A policy that will also include the obligation to change the access password regularly will be established and implemented.

Comments and recommendations of the Evaluation Committee
The Committee was informed that auditing of the use of personal data within the competence of the Ministry of Administration and Interior is in place. Log files are accessible only for data protection purposes; the Committee stresses the importance of respecting this principle.

As regards the IT security, the system seems to be robust and adequate in general. However, the quality of passwords should be improved, as the lengths and complexity (only alphanumeric symbols) are not sufficient. However, this is not a major concern, since the Committee was informed about plans to use for controlling the access smart cards, tokens and biometrics simultaneously with passwords. The Committee was informed about a Security Plan for N.SIS including organizational, personal, and technical measures; among them moving to a new building of the SIS National Centre in Bucharest which will locate the main and backup N.SIS servers and a new building of a Disaster Recovery Centre outside Bucharest. The Committee recommends not keeping backup files in the same building as the main system since this could create large risks. The Committee expects that reports on future developments will remove any doubt in this respect.

The Committee found clear and specific rules for the rights of access. The security system is in place and it is further developed. Critical operations are audited and audit trails are available to administrators and indirectly to the NSAPDP. The Committee was not able to verify periodical or random checks; only security incidents are monitored. The Committee recommends Romania to perform those checks - either both by the controller and the NSAPDP or by the NSAPDP only - as the authorities deem it useful. The use of mobile terminals in N.SIS seems to be a weak point. This has nevertheless been remedied by the set of compensatory measures. The use of TETRA standard is accepted as adequate. The Committee invites Romania to fully align its practice with the international standards in the field of information security.

Comments of Romania
As far as the recommendation concerning not keeping N.SIS backup files in the same building as the main system, we would like to inform the Committee that this recommendation will be considered by the Romanian authorities. The Security Plan for N.SIS will establish the location and the security measures necessary for keeping and handling backup files.

Concerning the alignment of Romanian practice with international standards in the field of information security, we would like to inform the Committee that all the national IT systems that will be in connection with SIS, including N.SIS, are upgraded, developed and implemented on the basis of principles derived from international standards in the field of information security. The NISA and N.SIS will be developed according to the SIS II Catalogue.

7. Visa applications

In the future, the consular posts of Romania will have on-line access to consult through NS-VIS system the SIS data (the national copy of CS.SIS) and national data (NISA database). Querying article 96 data from NISA database and from the national copy of CS.SIS through NS-VIS system will be realized simultaneously through an interface offered by NISA, based on WEB services.

The NS-VIS will be a web-based application. Data request by the NS-VIS application to SIS will be done automatically by the application program. Access to SIS data will be made through the application only by the user who implements a visa application.

Clients abroad (consulates, diplomatic missions, etc.) will open working sessions through INTERNET on a secured channel (encrypted tunnel) and will be served by a WEB Server with Application Server role, which will assure the second encryption level (software), as well as authorizing access to the system. The consulates' users that are accessing SIS data using fixed stations will be certified and authorized based on digital certificates (Public Key Infrastructure - PKI). Physical access to the offices will be monitored by control access system with access rights and protection officers.

Comments and recommendations of the Evaluation Committee
The Committee noted that the written disclaimer at the end of the visa application form does not seem to be intended to serve data protection purposes, as it is not in compliance with the requirements of article 12 (1) lit. c. of Law 677/2001 to inform the data subject inter alia about the recipients of the data and the data subjects' rights and the procedures to exercise these rights. Although it was informed that additional information fully compliant with the law is in each case provided orally at the reception desk of the respective consulate, as set out in the respective handbook, the Committee realizes that the instructions on how to inform the data subjects when applying for a visa abroad, however, merely repeat the legal provisions without providing further guidance to the consular staff in order to assure accuracy and exhaustiveness of the information provided orally. The Committee recommends that clear information is given to the subjects in writing (in addition to the disclaimer in the application form), at least at consular departments which are heavily used (such as Kishinev).

As to the visa issuing process, the Committee was satisfied when informed that the local staff is excluded from the execution of the key activities of the visa process. The security measures adopted include backups to the network connections between the consular posts and the Ministry of Foreign Affairs. The Committee would like to receive more information on how the recommendations made by the NSAPDP based on the findings of the inspections carried out in Consular Departments were implemented in practice.

Comments of Romania
Romania took note of the Committee's comments regarding the written disclaimer of the visa application form and informs the Committee that, starting with March 2010 when the Community Code on Visas will be implemented, Romania will fully apply its provisions and the present disclaimer will be amended, in accordance with Annex I- the visa application, from the Community Code on Visas.

Romania will make the necessary arrangements, as recommended by the Committee, so that information be disseminated to data subjects, in compliance with the provisions and requirements of article 12 (1) lit. c of Law 677/2001 on the protection of individuals concerning personal data processing and the free movement of such data.

After the two inspection missions made by the National Supervisory Authority for Personal Data Processing (NSAPDP) during November 2008, to the Romanian diplomatic missions in Kishinev and Belgrade, the Ministry of Foreign Affairs received and analyzed its recommendations and sent internal subsequent instructions not only to the two inspected missions, but also to the whole network of diplomatic missions and consular posts.

8. Public awareness

In order to increase the level of public awareness and information with regard to data protection, the NSAPDP has carried out a series of specific activities. It has initiated awareness campaigns in relation to data controllers' obligations as well as data subjects' rights, according to the Schengen Convention. Thus, both in the capital and in the country, seminars and workshops were organized, with representatives of the authorities involved in Schengen accession participating. During these meetings, promotional materials (brochures, guides, flyers) were distributed and press conferences (which are reflected in the media by articles in the press, interviews to the radio and TV) organized.

The supervisory authority's website: www.dataprotection.ro has been launched in March 2006 and represents an important tool for public information. It contains information on community and national legislation in the area of personal data protection, notification forms issued in order to standardize the notifications, a guide on filling in the forms to support data controllers, draft decisions and procedures, the structure and contact data of the authority, as well as other information of public interest. On this site, a special section was created, entitled SCHENGEN, which contains the Community legislation in the field, specific domestic legislation and a description of the goal and attributions of the Joint Supervisory Authority on Schengen (JSA). Moreover, in order to better keep the public informed with regard to the activities of the NSAPDP, its yearly activity report is published on its site.

A Guide concerning the *Schengen Information System* and *the personal data protection* was posted on the website and distributed inter alia among the police bodies.

The establishment of the front office desk and of the phone line represents another way to support data subjects and data controllers, namely by providing prompt information as to the specific rights of data subjects and the obligations of data controllers. In order to continue and improve the actions already taken, the NSAPDP has drafted a "Schengen Communication Strategy for 2008-2009".

Comments and recommendations of the Evaluation Committee

The Committee highly appreciates the extensive data protection awareness campaign which has proven effective - resulting i.a. in the rising number of requests addressed to the NSAPDP.

Both the NSAPDP and the Ministry of Administration and Interior have made considerable efforts to contribute to a multi-format awareness campaign on the rights of data through leaflets, media, and websites.

Comments of Romania

No comments needed.

9. International Cooperation

According to the provisions of Law no. 677/2001, the NSAPDP shall cooperate with similar authorities from abroad for mutual assistance, in order to guarantee the fundamental rights and freedoms that can be affected through the processing of personal data.

As to cooperation between supervisory authorities, the NSAPDP will act taking into account the basic principles established by the Joint Supervisory Authority, while drawing up harmonized proposals for joint solutions to existing problems.

Once Romania accedes to the Schengen area, the competent authorities will enforce the final decisions taken by foreign authorities or courts of another contracting party. Since Romania is not a full-fledged Schengen Member State yet, Romania has so far not received such court decisions passed by the competent judicial authorities of the other Member States which aim at reviewing, deleting or receiving of information, or obtaining damages related to an alert introduced into SIS.

Comments and recommendations of the Evaluation Committee

As far as international cooperation is concerned, the active participation of the NSAPDP in all relevant EU structures is traceable and identifiable in the activities performed and results achieved by the Authority. The acceptance of shared values regarding the processing of personal data by law enforcement authorities is evident also in the Ministry of Administration and Interior, while there is still room for improvement within the sphere of competence of the MFA.

Comments of Romania

Lawful processing of personal data is recognized as being of high importance for all the Romanian authorities and we will continue the efforts in order to ensure an appropriate level in this respect.

10. General conclusion

The Committee is of the opinion that Romania is well under way in preparing to accede to the Schengen acquis. The legal framework is largely in place and is expected to be completed by the end of this year with the adoption of two relevant laws related to Schengen and data protection (in May and September respectively). The supervisory practice is well in place though with regard to Schengen periodical or random checks on logs should be introduced. The NSAPDP is an independent body which has achieved an important status over the last years and hopefully the necessary resources will be in place by the time of accession to Schengen. The Committee invites Romania to develop a balanced system of enforcing information security systems.

ANNEX I

Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed

The Romanian Parliament adopts the present law.

Chapter I: General Provisions

Article 1: Purpose
(1) The purpose of this law is to guarantee and protect the individual's fundamental rights and freedoms, especially the right to personal, family and private life, with regard to the processing of personal data.
(2) The exercise of the rights stated by this law shall not be restricted except for the specified and limited cases stated by this law.
Article 2: Scope
(1) The present law applies to personal data processing, performed, totally or partially, through automatic means, as well as to the processing through means other than automatic ones, which are part of, or destined to, a personal data filing system.
(2) The present law applies to:
a) personal data processing, carried out within the activities of data controllers established in Romania;
b) personal data processing, carried out within the activities of Romanian diplomatic missions or consular offices;
c) personal data processing, carried out within the activities of data controllers not established in Romania, by using any means on Romanian territory, unless these means are only used for transiting the processed personal data through Romanian territory.
(3) In the circumstance referred to in paragraph (2) letter c), the data controller must designate a representative which must be a person based in Romania. The provisions of this law, applicable to the data controller, are also applicable to his representative, without prejudice to legal actions which could be initiated before a court of law against the controller himself.
(4) The present law applies to the processing of personal data, carried out by Romanian or foreign natural or legal persons of public or private law, regardless of the fact that the data processing takes place in the public or private sector.
(5) Within the limitations set out by the present law, it also applies to the processing and transfer of personal data, carried out within the activities of preventing, investigating and repressing criminal offences and maintaining public order, as well as other activities in the field of criminal law, with the limitations and restrictions imposed by law.
(6) The present law does not apply to personal data processing, carried out by natural persons exclusively for their use, if the data in question is not intended to be disclosed.
(7) The present law does not apply to personal data processing and the transfer of personal data, carried out within the activities in the field of national defense and national security, with the limitations and restrictions imposed by law.
(8) The provisions of this law do not infringe upon the obligations assumed by Romania through its ratified international legal instruments.

Article 3: Definitions
For the purposes of this law, the following terms are defined as follows:
a) personal data: - any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity;
b) personal data processing: - any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction;
c) storage: - keeping the collected personal data on any type of storage support;
d) personal data filing systems: - any organized personal data structure which may be accessed according to some specific criteria, regardless of the fact that this structure is distributed according to functional or geographical criteria;
e) data controller: - any natural or legal person, including public authorities, institutions and their legal bodies, that establishes the means and purpose of the personal data processing; if the purpose and means of the personal data processing is set out or based on a legal provision, the data controller shall be the natural or legal person assigned as data controller by that specific legal provision;
f) data processor: - a natural or legal person, of private or public law, including public authorities, institutions and their legal bodies, which processes personal data on the data controller's behalf;
g) third party: - any natural or legal person, of private or public law, including public authorities, institutions and their local bodies other than the data subject, than the controller, or the processor who, under direct authority of the controller or of his processor, is authorized to process data;
h) recipient: - any natural or legal person, of private or public law, including public authorities, institutions and their local bodies, to whom the data are disclosed, regardless of the fact that it is a third party or not; the public authorities which receive data in accordance with a special type of inquiry competence will not be considered consignees;
i) anonymous data: - data that, due to its specific origin or specific manner of processing, cannot be associated to an identified or identifiable person.

Chapter II: General Rules on Personal Data Processing

Article 4: Characteristics of Personal Data
(1) Personal data which are intended to be processed must be:
a) processed fairly and in accordance with the existing legal provisions;
b) collected for specific, explicit and legitimate purposes; further processing of personal data for statistical, historical or scientific research, will not be considered incompatible with the purpose they were initially collected for, if it is carried out according to the provisions of this law, including those referring to the notification submitted to the supervisory authority, as well as according to the guarantees regarding personal data processing, set out by the legal provisions on statistics' activity or the historical or scientific research;
c) adequate, pertinent and non excessive in relation to the purpose for which they are collected and further processed;

d) accurate and, if necessary, updated; for this purpose, appropriate measures shall be taken in order to erase and/or rectify inaccurate or incomplete data, from the point of view of the purpose for which they were collected and later processed;
e) stored in such a manner that allows the identification of the data subject only for the time limit required to fulfill the purposes for which they are collected and later processed; the storage of data for a longer period of time than the one mentioned, for statistical, historical or scientific research purposes, shall be carried out in accordance with the guarantees regarding personal data processing, provided in the relevant legal framework, and only for the period of time required to achieve these purposes.
(2) Data controllers have the obligation to observe the provisions of paragraph (1) and to ensure the implementation of these provisions by the data processor.

Article 5: Conditions of Legitimacy Regarding the Data Processing
(1) Any personal data processing, except for the processing which refer to the categories mentioned in Article 7 paragraph (1) and Articles 8 and 10, may be carried out only if the data subject has given his/her express and unequivocal consent for that processing.
(2) The data subject's consent is not required in the following situations:
a) when the processing is required in order to carry out a contract or an agreement previous to that contract to which the data subject is party of, or in order to take some measures, at his request, before signing that contract or previous agreement;
b) when the processing is required in order to protect the data subject's life, physical integrity or health or that of a threatened third party;
c) when the processing is required in order to fulfill a legal obligation of the data controller;
d) when the processing is required in order to accomplish some measures of public interest or regarding the exercise of public official authority prerogatives of the data controller or of the third party to which the date are disclosed;
e) when the processing is necessary in order to accomplish a legitimate interest of the data controller or of the third party to which the date are disclosed, on the condition that this interest does not prejudice the interests, or the fundamental rights and freedoms of the data subject;
f) when the processing concerns data which is obtained from publicly accessible documents, according to the law;
g) when the processing is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing;
(3) The provisions of paragraph (2) do not infringe the legal texts that govern the obligations of public authorities to respect and protect intimate, family and private life.

Article 6: Ending the Processing Operations
(1) At the end of the data processing operations, if the data subject has not given his/her express and unequivocal consent for another destination, or for further processing, the personal data shall be:
a) destroyed;
b) transferred to another data controller, provided that the former data controller guarantees the fact that the processing will have similar purposes to those of the former personal data processing;
c) transformed into anonymous data and stored exclusively for statistical, historical or scientific research;

(2) In the case of processing operations performed under the terms stated under Article 5 paragraph (2) letters c) or d), within the activities described under Article 2 paragraph (5), the data controller may store the personal data for the required period of time, in order to achieve the specific followed goals, under the condition that adequate measures are ensured in order to protect the data, and shall proceed afterwards to their destruction if the legal provisions on archive preservation are not applicable.

Chapter III: Special Rules on Personal Data Processing

Article 7: Processing Special Categories of Data

(1) Processing personal data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life, is prohibited.

(2) The provisions of paragraph (1) do not apply in the following situations:

a) when the data subject has expressly given his/her consent for such data processing;

b) when the processing is required in order to meet the obligations or specific rights of the data controller in the field of labor law, in accordance with the legal guarantees; a possible disclosure to third party of the processed data may take place only if the data controller is legally required to do so, or if the data subject has expressly agreed to the disclosure;

c) when the processing is required in order to protect the data subject's life, physical integrity or health or that of another person which is legally or physically unable to express his/her consent;

d) when the processing is carried out as part of the legitimate activities of a foundation, association, or of any other non-profit organization with a political, philosophical, religious or trade-union profile, provided that the data subject is a member of that organization or has regular contacts with the organization in its activity profile, and provided that the data shall not be disclosed to a third party without the data subject's consent;

e) when the processing refers to data expressly made public in a clear way by the data subject;

f) when the processing is required in order to ascertain, exert or defend a right in a court of law;

g) when the processing is required for preventive medical care, to establish a medical diagnosis, to provide medical care or treatment in the interest of the data subject, or to manage health services that are in the best interest of the data subject, on the condition that the processing of that data is performed by, or under the supervision of medical staff pledged to professional secrecy or by or under the supervision of another person subject to a similar obligation regarding the secrecy;

h) where there is a specific legal provision, regarding the protection of an important public interest, on the condition that the processing is carried out in compliance with the rights of the data subject and other legal guarantees provided by the present law.

(3) The provisions of paragraph (2) do not infringe the legal texts that govern the public authority's obligation to respect and protect intimate, family and private life.

(4) The Supervisory authority may decide, based on justified grounds, the prohibition of the processing of data belonging to the categories stated in paragraph (1), even if the data subject has given his/her written, unequivocal consent, and the consent has not been withdrawn, on the condition that the prohibition stated in paragraph (1) should not be eliminated by one of the cases referred to in paragraph (2) letters b) – g).

Article 8: Processing of Personal Data with an Identification Function

(1) The processing of the personal identification number or of other personal data with a general identification function may be carried out only if:

a) the data subject has given his/her express and unequivocal consent; or

b) the processing is expressly stated by a legal provision.

(2) The supervisory authority may establish other situations in which the processing of data stated in paragraph (1) may be carried out, only after adequate guarantees have been provided in order to observe the data subject's rights.

Article 9: Processing Personal Data Regarding the State of Health

(1) Except for the cases stated in Article 7 paragraph (2), the provisions of Article 7 paragraph (1) do not apply to the processing of health data in the following situations:

a) if the processing is necessary for the protection of public health;

b) if the processing is necessary for the prevention of an imminent danger, the prevention of a criminal offence or the prevention of the result of such an action or for the removal of the damaging results of such an action.

(2) The processing of health data may be carried out only by, or under the supervision of, medical staff who are under a pledge of professional confidentiality, except for the cases when the data subject has given, in writing, his/her unequivocal consent and as long as the consent has not been withdrawn, as well as except for the cases when the data processing is necessary for the prevention of an imminent danger, the prevention of a criminal offence or the prevention of the result of such an action or for the removal of the damaging results of such an action.

(3) The medical staff, health institutions and their staff may process personal health data without the authorization of the supervisory authority only when the data processing is required in order to protect the data subject's life, physical integrity or health. When the mentioned purposes refer to other people or to the general public and the data subject has not given his/her written and unequivocal consent, the preliminary authorization of the supervisory authority must first be demanded and obtained. The processing of personal data is forbidden beyond the limits of the authorization.

(4) Except for emergency reasons, the authorization provided under paragraph (3) may be given only after consulting the Romanian Medical College.

(5) Personal health data may only be collected from the data subjects themselves. Exceptionally, these data can be collected from other sources only when it is required in order not to compromise the processing's purpose, and when the data subject cannot or doesn't wish to provide them.

Article 10: Processing Personal Data Regarding Criminal Offenses or Infringements

(1) Processing personal data regarding criminal offenses committed by the data subject, or regarding previous criminal convictions, security measures or administrative or minor offense sanctions applied to the data subject, may be carried out only under the control of public authorities, within the limits of their powers given by law and under the terms established by the specific provisions in this field of law.

(2) The supervisory authority may establish other cases in which the data processing stated under paragraph (1) may be carried out, only on the condition that adequate guarantees are put in place to observe the rights of the data subject.

(3) A complete record of criminal convictions may be kept only under the control of a public authority, within its attributions, stated by law.

Articles 11: Exemptions
The provisions of Articles 5, 6, 7 and 10 do not apply to the situation in which the data processing is carried out exclusively for journalistic, literary or artistic purposes, or if the processing regards personal data that were expressly made public in a specific manner by the data subject or by the public character of the events that have taken place.

Chapter IV: The Rights of the Data Subject in the Context of Personal Data Processing

Article 12: Informing the Data Subject
(1) When personal data are obtained directly from the data subject, it is the data controller's obligation to provide the data subject the following information, except for the situations in which he/she already has this information:
a) the identity of the data controller and, if required, of the data controller's representative;
b) the purpose of the data processing;
c) additional information, such as: the recipients, or the categories of recipients of the data; whether the requested information is compulsory, and the consequences of the refusal to provide it; the existence of the data subject's rights, stated by this law, notably the right of access, intervention and objection as well as the terms in which they may be exerted;
d) any other information which may be expressly requested by the supervisory authority, considering the processing's specific situation.
(2) When the data are not obtained directly from the data subject, it is the data controller's obligation, at the moment of collecting data or at least before the first disclosure takes place, if he has the intention to disclose the data to a third party, to provide the data subject with the following minimum information, unless the data subject already possesses that information:
a) the identity of the data controller and, if required, of the data controller's representative;
b) the purpose of the data processing;
c) additional information, such as: the recipients, or the categories of recipients of the data; whether the requested information is compulsory, and the consequences of the refusal to provide them; the existence of the data subject's rights, stated by this law, notably the right of access, intervention and objection as well as the terms in which they may be exerted;
d) any other information which may be expressly requested by the supervisory authority, considering the processing's specific situation.
(3) The provisions of paragraph (2) do not apply when the processing of data is carried out exclusively for journalistic, literary or artistic purposes, if their enforcement might reveal the source of information;
(4) The provisions of paragraph (2) do not apply when the processing of data is carried out for statistical, historical or scientific research, or in any other situations if providing such information proves to be impossible or would involve a disproportional effort towards the legitimate interest that might be damaged, as well as in the situations in which recording or disclosure of the data is expressly stated by law.

Article 13: The Right of Access to Data
(1) Every data subject has the right to obtain from the data controller, upon request, and free of charge, once a year, the confirmation of the fact that the data concerning him/her are or are not being processed by the data controller. The data controller, in case he has processed any personal data concerning the petitioner, is obliged to communicate to the petitioner, along with the confirmation, at least the following:

a) information regarding the purposes of the data processing, the categories of data concerned, and the recipients or the categories of recipients to whom the data are to be disclosed;
b) communication in an intelligible form of the processed data and of any other available information regarding the source of origin of the respective data;
c) information on the technical principles and mechanisms involved in the data processing concerning that data subject;
d) information concerning the existence of the right of intervention upon the data, and the right to object, as well as the conditions in which the data subject can exert these rights;
e) information on the possibility of consulting the Register of personal data processing, stated under Article 24, before submitting a complaint to the supervisory authority, as well as to dispute the data controller's decisions in court, according to the provisions of this law;
(2) The data subject may request from the data controller the information stated under paragraph (1) through a written, dated and signed petition. The petitioner may underline his desire to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidential receipt of the information.
(3) It is the data controller's obligation to communicate the requested information, within 15 days of receipt of the petition, while complying with the petitioner's option as provided in paragraph (2).
(4) Regarding personal health data, the petition mentioned in paragraph (2) may be filled in by the data subject him/herself, or by medical staff who will mention the person on whose behalf the request has been made. Upon the data controller's or the data subject's request, such communication as mentioned in paragraph (3) may be carried out by a member of the medical staff, appointed by the data subject.
(5) If the personal health data are processed for scientific research purposes, if the risk of infringing the rights of the data subject does not exist and if the data are not to be used in order to take measures against a person, the communication mentioned in paragraph (3) may be dispatched within a period of time longer than the one mentioned in that paragraph, if that might affect the process or the outcome of the research, but it should not be delayed after the research has been completed. Such a situation is only allowed if the data subject has given his/her express and unequivocal consent for the data to be processed for the purpose of scientific research, as well as for the possible delay of the communication mentioned in paragraph (3);
(6) The provisions of paragraph (2) shall not apply when the processing of personal data is carried out exclusively for journalistic, literary or artistic purposes, if their application might affect confidentiality as to the source of the information.

Article 14: The Right of Intervention upon the Data
(1) Every data subject has the right to obtain from the data controller, upon request, and free of any charge:
a) as the case may be, rectification, updating, blocking or deletion of data whose processing does not comply with the provisions of the present law, notably of incomplete or inaccurate data;
b) as the case may be, transforming into anonymous data the data whose processing does not comply with the provisions of the present law;
c) notification to a third party to whom the data were disclosed, of any operation performed according to letters a) or b), unless such notification does not prove to be impossible or if it does not involve a disproportionate effort towards the legitimate interest that might thus be violated.
(2) In order to exert the right stated in paragraph (1), the data subject shall fill in a written, dated and signed petition. The petitioner may state his/her wish to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidential receipt of the information.

(3) The data controller has the obligation to communicate the measures taken, based on the provisions of paragraph (1), as well as, as the case may be, the name of a third party to whom the data concerning the data subject were disclosed, within 15 days from the date of the petition's receiving, whilst complying with the petitioner's possible option, according to paragraph (2).

Article 15: The Right to Object

(1) The data subject has the right to object at any moment, based on justified and legitimate reasons linked to his particular situation, to a processing of data regarding him/her, unless there are contrary specific legal provisions. In case of justified opposition, the processing may no longer concern the respective data.
(2) The data subject has the right to object at any moment, free of charge and without any justification, to the processing of the data concerning his/her person for overt marketing purposes on behalf of the controller or of a third party, or to be disclosed to a third party for such a purpose.
(3) In order to exercise the rights stated under paragraphs (1) and (2), the data subject shall fill in and submit to the data controller a written, dated and signed petition. The petitioner may specify if he/she wishes to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidentiality.
(4) The data controller has the obligation to inform the data subject of the measures taken, based on the provisions of paragraph (1) or (2), as well as, as the case may be, the name of the third party to whom the data concerning the data subject were disclosed, within 15 days of the date of the petition's arrival, in compliance with the petitioner's option, according to paragraph (3).

Article 16: Exemptions

(1) The provisions of Articles 12, 13, Article 14 paragraph (3) and Article 15 do not apply for such activities as mentioned in Article 2 paragraph (5), if their enforcement affects the efficiency of the action or the objective followed in order to fulfill the legal obligations of the public authority.
(2) The provisions of paragraph (1) are applicable solely for the period of time necessary for the achievement of the goal intended by carrying out the activities mentioned in Article 2 paragraph (5).
(3) As soon as the reasons that justified the enforcement of paragraphs (1) and (2) no longer exist, the controllers who perform the activities stated by Article 2 paragraph (5) shall take all necessary measures in order to ensure the compliance with the data subject's rights.
(4) Public authorities shall make a record of such cases and inform periodically the supervisory authority on the way these cases have been solved.

Article 17: The Right Not to be Subject to an Individual Decision

(1) Any person has the right to demand and receive the following:
a) the withdrawal or the cancellation of a decision that produces juridical effects concerning him/her, adopted exclusively on a personal data processing basis, carried out through automatic means, destined to evaluate some aspects of his/her personality, such as professional competence, credibility, behavior or any other similar aspects;
b) re-evaluation of any decisions regarding him/her, that affect him/her in a significant manner, if the decision was adopted exclusively on a basis of data processing that meets the requirements stated under letter a).
(2) Respecting the other guarantees stated by the present law, a person may be subject to a decision of the nature mentioned in paragraph (1), only in the following situations:
a) the decision is taken in the context of entering into or carrying out a contract, on the condition that the request to close or to bring the contract to conclusion, filled in by the data subject, has been satisfied or that some adequate measures to safeguard his/her legitimate interest have been taken, such as arrangements allowing him/her the possibility of sustaining his point of view in order to guarantee the protection of its own legitimate interest;

b) the decision taken is authorized by a law which states the measures that guarantee the protection of the data subject's legitimate interests.

Article 18: The Right to Refer to a Court of Law

(1) Without prejudice to the possibility of addressing the supervisory authority, the data subject has the right to address to a court of law in defense of any rights, guaranteed by the present law, that have been infringed.

(2) Any person that has suffered a prejudice as a consequence of unlawful processing of personal data may address a competent court of law in order to obtain compensation for the prejudice suffered.

(3) The competent court of law is the one whose territorial jurisdiction covers the complainant's domicile. The complaint addressed to the court of law is exempt from stamp tax.

Chapter V: Confidentiality and Security of Processing

Article 19: Confidentiality of Data Processing

Any person who acts under the authority of the data controller or of the data processor, including the data processor, who has access to personal data, may process them only in accordance with the data controller's specific instructions, except when the above-mentioned person's actions are based on a legal obligation.

Article 20: Security of Data Processing

(1) It is the data controller's obligation to apply the adequate technical and organizational measures in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective processing involves the data's transmission within a network, as well as against any other form of illegal processing.

(2) These measures shall ensure, depending on the state of the art techniques employed and the costs, adequate security against processing risks as well as observing the nature of the data that must be protected. The minimum security requirements shall be issued by the supervisory authority and shall be periodically updated, according to the technological progress and the accumulated experience.

(3) When appointing a data processor, the data controller has the obligation to assign a person who presents sufficient guarantees regarding technical security and the organizational measures concerning the data to be processed, as well as the obligation to ensure that the assigned person complies with these measures.

(4) The supervisory authority may decide, in individual cases, that the data controller should adopt additional security measures, except such measures that regard the guaranteed security of telecommunication services.

(5) Data processing performed by an appointed data processor shall be initiated following a written contract which should necessarily contain the following:

a) the processor's obligation to act strictly in accordance with the instructions received from the data controller;

b) the fact that accomplishing the obligations set out in paragraph (1) also applies to the data processor.

Chapter VI: Supervising and Control Of Personal Data Processing

Article 21: The Supervisory Authority

(1) The supervisory authority, in the terms of the present law, is the National Supervisory Authority for Personal Data Processing.

(2) The supervisory authority carries out its activity completely independent and impartial.

(3) The supervisory authority shall monitor and control with regard to their legitimacy, all personal data processing, subject to this law. In order to achieve this purpose, the supervisory authority exerts the following attributions:

a) issues the standard notification forms and its own registers;

b) receives and analyses the notifications concerning the processing of personal data and informs the data controller on the results of the preliminary control;

c) authorizes personal data processing in the situations set out by law;

d) may dispose, if it notices the infringement of the provisions of the present law, temporarily suspending the data processing or ending processing operations, the partial or total deletion of processed data and may notify the criminal prosecution bodies or may file complaints to a court of law;

d^1) informs the natural or legal persons that work in this field, directly or through their associative bodies on the need to comply with the obligations and to carry out the procedures set out by this law;

e) keeps and makes publicly accessible the personal data processing register;

f) receives and solves petitions, notices or requests from natural persons and communicates their resolution, or, as the case may be, the measures which have been taken;

g) performs investigations –*ex officio*, or upon requests or notifications;

h) is consulted when legislative drafts regarding the individual's rights and freedoms are being developed, concerning personal data processing;

i) may draft proposals on the initiation of legislative drafts or amendments to legislative acts already enforced, in the fields linked to the processing of personal data;

j) collaborates with the public authorities and bodies of the public administration, centralizes and analyzes their yearly activity reports on the protection of individuals with regard to the processing of personal data, issues recommendations and assents on any matter linked to the protection of fundamental rights and freedoms regarding the processing of personal data, on request of any natural person, including the public authorities and bodies of public administration; these recommendations and assents must mention the reasons on which they are based and a copy must be transmitted to the Ministry of Justice; when the recommendation or assent is requested by the law, it must be published in the Official Journal of Romania, Part I;

k) co-operates with similar foreign authorities in order to ensure common assistance, as well as with foreign residents for the purpose of guaranteeing the fundamental rights and freedoms that may be affected through personal data processing;

l) fulfills other attributions set out by law;

m) the manner in which the National Supervisory Authority for Personal Data Processing is organized and functions is set out by law.

(4) The entire staff of the supervisory authority has the obligation of permanently keeping the professional secrecy, except for the cases set out by law, regarding the confidential or classified information they have access to in carrying out their duties, even after termination of their legal employment relations with the supervisory authority.

Article 22: The Notification Addressed to the Supervisory Authority

(1) The data controller is obliged to notify the supervisory authority, either personally or through a representative, before initiating any kind of data processing which has a similar or related purpose(s) to previous data processing activities.

(2) Notification is not necessary in the event that the sole purpose of the data processing is to keep a record available for public reference, open for consultation to the general public or to any person who proves a legitimate interest, provided that the data processing is strictly limited to such data that are necessary to the above mentioned record.

(3) The notification shall contain the following information:

a) the name, address or premises of the data controller and of his representative, as the case may be;

b) the purpose(s) of the data processing;

c) a description of the category/categories of the data subjects and of the data, or the categories of data, that are to be processed;

d) the recipients or the categories of recipients to whom the data is intended to be disclosed;

e) the guarantee accompanying the disclosure to a third party;

f) the manner in which the data subjects are informed of their rights, an estimate date on ending data processing operations and the future destination of the data;

g) transfers aboard of personal data intended to be carried out;

h) a general description that allows a preliminary assessment of the measures taken in order to ensure data processing security;

i) mention of any data filing system related to the processing, and of possible relation to other processing or other data recording systems, irrespective of the fact that they are situated on Romanian territory or not;

j) the reasons that justify the enforcement of the provisions of Articles 11 and 12 paragraph (3) or (4), or of Article 13 paragraph (5) or (6), in cases that the data processing is performed exclusively for journalistic, literary, artistic or statistical purposes, or for historical or scientific research.

(4) If the notification is incomplete, the supervisory authority shall demand its completion.

(5) Within its investigative powers, the supervisory authority may demand other information, notably regarding the data's origin, the automatic processing technology used and details about the security measures. The provisions of this paragraph do not apply in the situations in which the data is processed exclusively for journalistic, literary or artistic purposes.

(6) If the processed data is intended to be transferred abroad, the notification shall consist of:

a) the data categories subject to the transfer;

b) the country of destination for each data category.

~~(7) The notification is subject to a fee that must be paid by the data controller to the supervisory authority.~~ (abrogated by Law no. 278/2007)

(8) The public authorities that carry out personal data processing related to the activities described in Article 2 paragraph (5), based on the law or in compliance with the obligations assumed through ratified international agreements, are exempt from the fee set out in paragraph (7). The notification shall be sent within 15 days from the entering into force of the legislative act that sets out the obligation in case and shall only contain the following elements:

a) the name, address/premises of the data controller;

b) the purpose and the legal basis of the data processing;

c) the personal data categories subject to processing.

(9) The supervisory authority may establish other situations in which the notification is not required, other than those provided in paragraph (2), or situations in which the notification may be submitted in a simplified manner as well as the content of such a notification, in the following cases:

a) in situations in which, considering the nature of the data which are processed, the processing may not infringe, at least apparently, the rights of the data subject, on the condition that the purposes of that processing, the data or categories of processed data, the data subjects or categories of data subjects, the recipients or categories of recipients and the period for which the date are stored are all precisely mentioned;
b) in situations in which the processing is carried out in accordance with the provisions of Article 7 paragraph (2) letter d).

Article 23: Preliminary Control
(1) The supervisory authority shall establish the categories of processing operations that may present special risks for the person's rights and freedoms.
(2) If based on the notification, the supervisory authority assesses that the data processing belongs to one of the categories mentioned in paragraph (1), it shall decide on a preliminary control before the data processing in case begins, and accordingly informs the controller.
(3) The data controllers who have not been informed within 5 days of notification upon a preliminary control being ordered may start the data processing.
(4) In the situation provided in paragraph (2) the supervisory authority has the obligation, within no longer than 30 days from notification, to inform the data controller on the results of the control carried out, and on the decision issued thereupon.

Article 24: Personal Data Processing Record
(1) The supervisory authority keeps a personal data processing record, of the registered processing under the provisions of Article 22. The registry shall contain all the information set out Article 22 paragraph (3).
(2) Each data controller is given a registration number. The registration number must be mentioned on every document through which personal data are collected, stored or disclosed.
(3) Any change affecting the accuracy of the registered information will be communicated to the supervisory authority within 5 days. The supervisory authority will immediately make the necessary amendments to the register.
(4) The processing activities of personal data which started before the present law has come into force will be notified in order to be registered within 15 days of the date when the present law enters into force.
(5) The personal data processing register is available for public reference. The supervisory authority shall establish the accessibility procedures.

Article 25: Complaints Addressed to the Supervisory Authority
(1) In order to defend the rights set out by the present law, the persons whose personal data are processed under the terms of this law may file in a complaint to the supervisory authority. The complaint may be addressed directly or through a representative. The data subject may empower an association or a foundation to represent his/her interests.
(2) The complaint submitted to the supervisory authority is invalid if a claim, concerning the same matter and parties, was previously submitted to a court of law.
(3) Except for the cases in which a delay would cause imminent or irreparable damage, the complaint submitted to the supervisory authority cannot be addressed earlier than 15 days from submitting a similar complaint to the data controller.

(4) In order to solve the complaint the supervisory authority may, if considered necessary, hear the data subject's view, the data controller's view and the views of the empowered person or that of the association or foundation which represents the interests of the data subject. These persons have the right to file in the requests, documents and memoirs. The supervisory authority may order an expertise.
(5) If the complaint is considered to be grounded, the supervisory authority may decide upon any of the measures set out in Article 21 paragraph (3) letter d). Temporary interdiction of the data processing may be ordained only until the reasons that have determined such measures have ended.
(6) The decision must be grounded and shall be brought to the involved parties' attention within 30 days of registering the complaint.
(7) The supervisory authority may order, if necessary, some or all data processing operations to be suspended until the complaint has been solved, under the provisions of paragraph (5).
(8) The supervisory authority may address to a court of law in order to defend the rights of the data subjects as guaranteed by the present law. The competent court of law is the Court of Bucharest (second level). The complaint addressed to the court of law is exempted from stamp taxes.
(9) Upon request of the data subjects, for grounded reasons, the court may decide suspending the data processing until the supervisory authority solves the complaint.
(10) The provisions of paragraphs (4) to (9) also apply to the situation in which the supervisory authority acknowledges, by any other means, about a violation of the rights of the data subjects, as recognized by the present law.

Article 26: Appeals against the Decisions of the Supervisory Authority
(1) The data controller or the data subject may submit an appeal against any decision made by the supervisory authority based on the provisions of the present law, within 15 days from communication, under the sanction of the loss of right, to the competent administrative court. The matter is judged urgently after both parties have been called in front of court. The court's resolution is permanent and irrevocable.
(2) Personal data processing carried out within the activities set out in Article 2 paragraph (5) are exempted from the provisions of paragraph (1), and also of Articles 23 and 25.

Article 27: Exercising the Investigative Powers
(1) The supervisory authority may investigate *ex oficio* or as a result of a complaint, any infringement of the data subject's rights, of the controller's obligations and, as the case may be, those of the processors, in order to protect the fundamental rights and freedoms of the data subjects.
(2) The supervisory authority may not exercise its investigative powers in case a complaint was previously addresses to a court of law, concerning the same breach and parties.
(3) In the exert of its investigative powers, the supervisory authority may request any information linked to the processing of data from the data controller and may verify any document or record regarding the processing of personal data.
(4) The state and professional secret cannot be invoked in order to prevent the exercise of the supervisory authority's powers, set out by the present law. When the protection of the state or of the professional secret is invoked, the supervisory authority has the obligation to keep the respective secret.

Article 28: Rules of Conduct
(1) The professional associations have the obligation to elaborate and submit for approval, to the supervisory authority, codes of conduct that contain adequate rules in order to protect the rights of persons whose personal data may be processed by the members of the associations.

(2) The rules of conduct must contain measures and procedures able to ensure satisfactory protection, taking into account the nature of the data that may be processed. The supervisory authority may impose other specific measures and procedures for the period of time during which the rules of conduct are not adopted.

Chapter VII: The Transfer Abroad of Personal Data

Article 29: Conditions for the Transfer Abroad of Personal Data
(1) The transfer to another state of data that are subject to processing or are destined be processed after being transferred may take place only if the Romanian law is not infringed and the state of destination ensures an adequate level of protection.
(2) The protection level will be assessed by the supervisory authority taking into account all the circumstances in which the transfer is to be performed, especially the nature of the data to be transferred, the purpose and the period of time proposed for the processing, the state of origin and the state of final destination, as well as the legislation of the latter state. In case the supervisory authority notices that the protection level offered by the state of destination is unsatisfactory, it may ban the data transfer.
(3) Data transferred to another state shall always be subject to prior notification to the supervisory authority.
(4) The supervisory authority may authorize the data transfer to another state which does not offer at least the same protection level as the one offered by the Romanian legislation, provided that the data controller offers enough guarantees regarding the protection of fundamental individual rights. These guarantees must be established through contracts signed by the data controllers and the natural or legal person(s) who have offered the transfer.
(5) The provisions of paragraphs (2), (3) and (4) do not apply in case the data transfer is based on a special law or on an international agreement ratified by Romania, notably if the transfer is done to the purpose of prevention, investigation or repressing a criminal offense.
(6) The provisions of the present article do not apply when the data is processed exclusively for journalistic, literary or artistic purposes, if the data were made public expressly by the data subject or are related to the data subject’s public quality or to the public character of the facts he/she is involved in.

Article 30: Situations in which the Transfer is Always Allowed
The data transfer is always allowed in the following situations:
a) when the data subject has explicitly given his/her consent for the transfer; if the data transfer is linked to any of the data provided in Articles 7, 8 and 10 the consent must be written;
b) when it is required in order to carry out a contract signed by the data subject and the data controller, or to apply some pre-contractual measures taken upon the request of the data subject;
c) when it is required in order to sign or carry out a contract concluded or about to be concluded between the controller and a third party, in the data subject’s interest;
d) when it is necessary for the accomplishment of a major public interest, such as national defense, public order or national safety, carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court, on the condition that the data is processed solely in relation with this purpose, and only for as long as it is required;
e) when it is required in order to protect the data subject’s life, physical integrity or health;
f) when it is a consequence of a previous request for access to official documents that are open to the public or of a request for information that can be obtained from registers or any other documents of public access.

Chapter VIII: Infringements and Sanctions

Article 31: Failure to Notify and Malevolent Notification
Failure to submit the compulsory notification under the terms set out by Article 22 or Article 29 paragraph (3), as well as incomplete notification or one that contains false information, if the respective maladministration falls short of a criminal offense, are considered minor offenses liable to a fine of 5 million to 100 million ROL (Romanian currency – lei).
Article 32: Illegal Processing of Personal Data
The processing of personal data by a controller or by an empowered person of the data controller, breaching the provisions of Articles 4-19, or while disregarding the rights set out in Articles 12- 15 or in Article 17 is considered a minor offense if the respective maladministration falls short of a criminal offense and is fined from 10 million to 250 million ROL.
Article 33: Failure to Fulfill the Obligations Regarding the Confidentiality and Enforcement of Security Measures
Failure to fulfill the obligations regarding the enforcement of the security measures provided by Articles 19 and 20 and the confidentiality is a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 15 million to 500 million ROL.
Article 34: Refusal to Supply Information
The refusal to supply the requested information or documents to the supervisory authority in the exercise of his investigative powers set out by Article 27 is considered a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 10 million to 150 million ROL.
Article 35: Ascertaining Infringements and Applying Sanctions
(1) Ascertaining an infringement and applying sanctions are carried out by the supervisory authority, which may delegate these powers on to a member of staff and also by the empowered representatives of the bodies with supervising or control powers in their legal competence.
(2) The provisions of the present law regarding the infringements are complementary to those of the Government Ordinance No. 2/2001 on the legal framework of minor offenses, when the present law does not state otherwise.
(3) The minutes that report infringements and establish the sanctions may be appealed against in the administrative section of a court of law.

Chapter IX: Final Provisions

Article 36: Entering into force
The present law enters into force on the date of its publication issue in the Official Journal of Romania, Part I and will be enforced within three months of its entering into force.
The Senate adopted the present law during the session of the 15th of October 2001, in accordance with the provisions of Article 74 paragraph (2) of the Romanian Constitution.

President of the Senate
NICOLAE VĂCĂROIU
The present law was adopted by the Chamber of Deputies in the session of the 22nd of October 2001, in accordance with the provisions of Article 74 paragraph (2) of the Romanian Constitution.
President of the Chamber of Deputies
VALER DORNEANU
Published in the Official Journal of Romania, Part I, No. 790/12 December 2001

ANNEX II

LAW no. 102/2005
regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing

CHAPTER 1
GENERAL PROVISIONS

Article 1

(1) The National Supervisory Authority for Personal Data Processing, hereafter named *the National Supervisory Authority*, is set up as a public authority, autonomous and independent in relation with any other public authority, natural or legal person, with legal personality, exercising the attributions it has been invested with by the present law, as well as by the special laws regulating the activity of personal data processing and the free movement of the data.
(2) The National Supervisory Authority for Personal Data Processing aims at protecting the fundamental human rights and liberties of the natural persons, in particular the right to private and family life, with regard to personal data processing and free movement of these data.
(3) The National Supervisory Authority's powers and duties are set up by Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data.
(4) The National Supervisory Authority's headquarters is in Bucharest.

Article 2

(1) While carrying out its duties, *the National Supervisory Authority* is independent in relation with any other public authority and exercises its attributions in a transparent and impartial manner.
(2) While performing its duties, *the National Supervisory Authority* may not substitute to the public authorities.
(3) *The National Supervisory Authority* shall not be subject to any imperative or representative mandate or to instructions and dispositions from other authorities.

Article 3

(1) *The National Supervisory Authority* is headed by a President, whose position is similar to a Secretary of State, from the point of view of the representation, salary and ranking.
(2) The President heads the entire activity of the National Supervisory Authority and represents it in front of the Chamber of Deputies and Senate, in relation with the Government, ministries, other public administration authorities, organisations, as well as Romanian and foreign, natural and legal persons.
(3) While managing the National Supervisory Authority, the President is assisted by a vice/president, whose function is similar to the function of a Undersecretary of State, from the point of view of the representation, salary and ranking.
(4) The President of the National Supervisory Authority is main credit co-ordinator.
(5) While performing his duties, the President issues Decisions and Instructions mandatory for all institutions and units whose activity makes the object of the acts above mentioned.

(6) The Decisions and the Instructions with normative character are published in the Official Journal of Romania, Part I.
(7) The public authorities are compelled to communicate or, as the case may be, by law, to provide the National Supervisory Authority with the information, the documents or the acts they hold, related to the requests submitted to the National Supervisory Authority, supporting thus the Authority in exercising its duties.

Article 4
(1) The activity of the National Supervisory Authority's President, vice-president and the staff has a public character.
(2) Upon the request of the persons whose rights and liberties were prejudiced or due to wellgrounded
reasons, the National Supervisory Authority's President may decide for the confidential character of his activity.

Article 5
(1) The National Supervisory Authority's President submits yearly activity reports in the plenary session of the Senate. The reports shall contain information regarding the National Supervisory Authority's activity. They may contain recommendations regarding the legislation amendment or other measures aiming at the protection of the citizens' rights and liberties with regard to personal data processing.
(2) The yearly report is published in the Official Journal of Romania, Part II, after presenting it in the plenary session of the Senate.

CHAPTER 2
Appointing and dismissing the National Supervisory Authority's President and vice-president

Article 6
(1) The Senate, for a 5 years mandate appoints the National Supervisory Authority's President and vice-president. The President and vice-president's mandate can be renewed only once.
(2) The President or vice-president of the National Supervisory Authority shall be Romanian citizens, with a law degree from a high educational institution, under the law. The President and the vice-president must enjoy real independence, must have a good professional competence, a good reputation and a high civic probity.
(3) The presidency or vice-presidency of the supervisory authority is incompatible with any other public or private function, except for the academic ones.
(4) While exercising these functions, the president or vice-president of the supervisory authority can not be a member of political parties or other political structures and is not allowed to hold, directly or indirectly, shares of companies carrying out activities in fields under its responsibility.

Article 7
(1) The proposals regarding the candidates for President and vice-president shall be made by the Standing Bureau of the Senate, at the recommendation of the parliamentary groups of the two Chambers of the Parliament.

(2) The candidates shall submit to the Committee for legal affairs, appointment, ethics, immunity and validation within the Senate, the acts certifying that they do fulfil the conditions under law in order to exercise the presidency or vice-presidency of the national supervisory authority. The candidates will be interviewed by the Committee for legal affairs, appointment, ethics, immunity and validation. The Senate passes a judgment upon over the plenary hearing.
(3) The appointment of the President of the national supervisory authority is made with the majority vote of the senators. If during the first scrutiny the above mentioned majority is not reached, new elections must be organized and only the first two candidates of the previous scrutiny may participate.

Article 8
(1) The president and vice-president's mandate starts on the appointment date and lasts until the installation of the new president, respectively vice-president.
(2) Before starting the exercise of the mandate, the President of the national supervisory authority shall be sworn in before Senate:
"I swear to respect the Constitution and the law of the country, and to defend the rights and liberties of the citizens, carrying out my attributions as president of the national supervisory authority for the processing of personal data, in good faith and impartiality. So help me God!".
(3) The oath may be taken without the religious part.
(4) The refusal to take the oath prevents the president (the vice/president, respectively) of the national supervisory authority from starting her/his activity and opens the procedure for a new appointment.

Article 9
(1) The President's mandate, the one of the vice-president, respectively, ends before the expiration of it's term in case of resignation, revocation or incompatibility with other public or private functions, incapacity of carrying out the attributions for more than 90 days, attested by a medical examination, or death.
(2) The removal from office of the President or the vice-president of the national supervisory authority, as a result of infringing the Constitution and the laws or in case of failure to carry out his/her duties, shall be carried out at the proposal of the Standing Bureau of the Senate, on the basis of the report of the Committee for legal affairs, appointment, ethics, immunity and validation, with the majority vote of the senators.
(3) The resignation, incompatibility, incapacity of carrying out the attributions or the death shall be ascertained by the Standing Bureau of the Senate no later than 10 days from the appearance of the cause determining the ceasing of the mandate.

CHAPTER 3
THE ATTRIBUTIONS
OF THE NATIONAL SUPERVISORY AUTHORITY'S PRESIDENT

Article 10
The President of the National Supervisory Authority has the following attributions:
a) organizes and coordinates the activity of the National Supervisory Authority for the Personal Data Processing;
b) informs the operators and the data subjects of the rights and obligations incumbent to them and independently oversees the way of the legislation regarding the personal data processing and the free movement of such data is implemented;

c) informs the operators of their incumbent obligations and the individuals of their rights regarding the processing of personal data;
d) oversees the way of the legislation regarding the personal data processing and the free movement of such data is implemented;
e) receives and distributes the requests of individuals who have suffered damage as a result of the breach of the citizens' rights and freedoms regarding the personal data processing and the free movement of such data; and passes judgement upon these requests;
f) aims at the legal conclusion of the requests and requests to the natural and legal persons to stop violating the citizens' rights and freedoms, and to restore the petitioner's rights and repair the damages;
g) employs the National Supervisory Authority's personnel and exerts the administrative and disciplinary authority's right upon them.
h) exercises the function of principal credit coordinator (ordonnateur de crédites);
i) co-operates with similar national and international institutions;
j) fulfils the attributions requested by the present law, the special laws that govern the activity of personal data process and the free movement of such data and the Regulation on the organisation and functioning of the National Supervisory Authority.

Article 11
(1) The attributions of the vice-president of the National Supervisory Authority are set out in the Regulation on the organisation and functioning of the National Supervisory Authority.
(2) The vice-president of the National Supervisory Authority may exert the President's attributions in case of temporary incapacity.

Article 12
(1) The President of the National Supervisory Authority exerts the attributions ex officio or upon request of the persons who have suffered damage stipulated in art. 10, letters e) and f).
(2) The requests can be made by any individual, regardless of the citizenship, age, sex, political affiliation and religious belief and also by any legal person.

Article 13
(1) The National Supervisory Authority has the right to make personal investigations, to request the public administration authority the necessary information and documents for the investigation, to interrogate and to take declarations from the leaders of the public administration authority and from any other civil servant who can give the necessary information for solving the request addressed to the National Supervisory Authority regarding the personal data processing and free movement of these data.
(2) The provisions of the paragraph (1) apply to the other public authorities and institutions, public services under the authority of the public administration authority, as well as to the natural and legal persons subject to the legislation regarding the personal data processing and free movement of such data.

Article 14
(1) The President of the National Supervisory Authority and its personnel have access, under the law, to the secret documents held by the public authorities or other legal persons, in the degree they are deemed necessary in order to exert his attributions, under law.
(2) The president of the National Supervisory Authority and its personnel are bound not to divulge or make public the information or secret documents they had had access to. This obligation is maintained even after the person concerned has ceased its activity within the National Supervisory Authority, under the sanction provided by criminal law.

CHAPTER 4
THE ORGANISATION AND FUNCTIONING OF THE NATIONAL SUPERVISORY AUTHORITY

Article 15

(1) The organisational structure of the National Supervisory Authority is approved by its President, with the approval of the Standing Bureau of the Senate.

(2) The maximum number of positions, except the dignitaries, is 50. Until the budget recalculation for 2005, the National Supervisory Authority will have 37 positions, except the dignitaries.

(3) The Regulation for organisation and functioning is drafted by the National Supervisory Authority, and it is approved by the Standing Bureau of the Senate.

(4) The payroll and the structural departments are approved by the National Supervisory Authority's President.

Article 16

(1) The National Supervisory Authority's staff consists of civil servants or hired personnel, appointed after examination, under law.

(2) The National Supervisory Authority's staff attributions, tasks and personal liabilities are set up by the job description, in accordance with the provisions of the Regulation for organisation and functioning.

(3) The employment, promotion, as well as the modification and cessation of the activity of the National Supervisory Authority's hired personnel is approved by the President's Decision, in accordance with the law.

(4) The National Supervisory Authority's employees can not hold shares of companies carrying out activities in fields under its responsibility and can not be members of those companies' management boards.

(5) Breaching the provisions of this law, of the special laws ruling this field of activity or the National Supervisory Authority's Regulation for the organisation and functioning entails criminal, disciplinary and administrative liability, on a case by case basis.

Article 17

(1) The National Supervisory Authority has it's own budget, stipulated as a distinct part of the state budget.

(2) The draft budget is elaborated by the National Supervisory Authority and it is submitted to the Government in order to be included distinctly in the draft state budget. The President's objections to the draft budget elaborated by the Government are submitted to the Parliament in order to be solved.

Article 18

The National Supervisory Authority's payroll is elaborated, under law, in accordance with the similar structure of the two Chambers of Parliament.

CHAPTER 5
FINAL AND TRANSITORY DISPOSITIONS

Article 19
(1) The entire data base, including the archive and all other documents regarding the protection of personal data, held and managed by The People's Advocate will be submitted to the National Supervisory Authority, in accordance with a "take over protocol" due to be carried out in 45 days after the present law enters into force.
(2) When the time frame set up in paragraph (1) is fulfilled, the National Supervisory Authority shall take over the entire activity regarding the protection of personal data, as well as the staff carrying out this activity, from the People's Advocate.
(3) Until the time frame set up in paragraph (1) is fulfilled, the Government shall provide the National Supervisory Authority with headquarters and all other facilities required, in order to ensure its proper functioning.
(4) After the Regulation mentioned in article 15 paragraph (3) is adopted, but no longer after the time frame set up in paragraph (1), the National Supervisory Authority will hire the required staff, in order to properly fulfil its legal attributions.
► *Chapter 5 of Law No. 102/2005, Article 19, paragraph (1) was amended by Governemt's Ruling No. 131/2005: the time frame set up in paragraph (1) was delayed until 31st of December 2005.*

Article 20
(1) The 37 positions and the necessary funds required by the functioning of the National Supervisory Authority will be ensured by the appropriate deduction of them from the People's Advocate number of positions and funds.
(2) The Ministry of Public Finance will bring the necessary modifications to the state budget, as required by the provisions of paragraph (1), as well as to the budgets and annexes of the People's Advocate and the National Supervisory Authority.

Article 21
Until the time frame set up in article 19, paragraph (1) is reached, the People's Advocate will carry out its legal attributions regarding the protection of personal data.

Article 22
Law no. 677/2001 on individuals protection with regard to personal data processing and free movement of these data, published in the OJ, part I, no. 790/12.12.2001 is amended as follows:
1. Article 21 paragraph (1) shall provide:
"Article 21

(1) The supervisory authority, as provided by the this law, is the National Supervisory Authority for Personal Data Processing."
2. Article 21, paragraph (3) is amended with a new letter, letter d1, as follows:
" d1) Informs individuals and companies in this field of activity of their legal requirements, as set out by this law."
3. Article 21, paragraph (3) is amended with a new letter, letter m, as follows:
"m) The organisation and functioning of the National Supervisory Authority for Personal Data Processing are established by law."
4. Article 27, paragraph (5) is annuled.

Article 23
The Declaration set out in Article 2, paragraph (3) of Law No.682/2001 regarding the ratification of the Convention on the individuals' protection with regard to personal data automatic processing, adopted in Strasbourg on 28.01.1981, published in OJ, part I, no. 830/21.12.2001, is amended as follows:
"Article 3, paragraph (2), letter c):
The present Convention is applied also to personal data processing carried out in other ways than automatic ones, which are part of a recording system or which are to be included in such a system.
The competent national authority is the National Supervisory Authority for Personal Data Processing."

Article 24
From the date of the entering into force of the present law, the Standing Bureau of the Senate will sent its proposals for the candidates to the National Supervisory Authority for Personal Data Processing's President position to the Committee for Legal Affairs, Appointment, Ethics, Immunity and Validation, , in no longer than 10 days, according to article 7 of this law.
This law was adopted by the Romanian Parliament in accordance with the provisions of articles 75 and 76 paragraph (1) of the Romanian Constitution.

ANNEX III

Government Emergency Ordinance no. 128/2005 on setting up, organizing and function of the National IT System on Alerts

Romania's Official Journal No.866/26 September 2005

Having regard of
the utmost importance of setting up, at national level, of an IT system SIS II compatible, in the context of the need to ensure border security, which represents a fundamental requirement for Romania's EU accession and, in case of non-accomplishment, it could activate the safeguard clause,

Having regard that
any delay in adopting the necessary legal framework would raise problems, on one hand, in setting up the institutional framework and the technical facilities of the IT system, and on the other hand, in adopting the subsequent legislation that establishes the guiding lines and the working mechanism of the system,

With a view to respecting the calendar of measures assumed under 2005 Revised Schengen Action Plan.

Having regard that
all the abovementioned elements are of public interest and represent exceptional situations, the clarification of their legal framework is compulsory.

In base of art 115 paragraph 4 of the Romanian Constitution, republished,

The Romanian Government adopts the present emergency ordinance:

CHAPTER I
GENERAL FRAMEWORK

Art.1

(1) The National IT System on alerts, herein referred to as NISA, was set up as a prior step in the process of Romania's accession to the Convention Implementing the Schengen Acquis of 14th of June 1985, herein referred to as CISA.

(2) Upon Schengen Accession, the NISA allows the competent authorities to get access to hits on persons and goods through an automatic search procedure with a view to accomplish their relevant responsibilities on border trespassing control, respecting the custom's regime, visa issuing and residents permits provisions, and other checks and specific activities done by the police bodies or by other competent authorities with a view to ensure the public order and safety.

(3) On Romania's accession to the Schengen Agreement, NISA will provide data to SIS, according to the European provisions in the field.

Art.2

In terms of definitions, the following words and expression must be understood as follows:

(a) hits – data relative to persons and/or goods identified or identifiable that must be the object of certain measure disposed by a competent authority, according to law provisions with a view to respecting the public interest, the free movement of persons and goods or, if needed, to ensuring the order and public safety;

(b) competent authorities – authorities with responsibilities in supplying and/or consulting the hits contained in NISA, foreseen by art.5;

(c) transaction – any kind of insertion, alteration or deletion of the alerts contained in the NISA.

(d) Schengen IT System – technical support of the common IT system set up by CISA.

CHAPTER II
COMPETENT AUTHORITIES IN THE ADMINISTRATION AND EXPLOITATION OF THE NISA

Art. 3

(1) Ministry of Administration of Interior is the public central authority that manages and ensures the good functioning of the NISA, the integrity of the hits contained by it and the process of data insertion into SIS, according to the requirements of the Schengen acquis.

(2) From the technical point of view, SINS is managed by the IT/C central structure within MoAI with responsibilities in the field.

(3) The Committee for Strategic Coordination, herein referred to as CCS, an organism with analysis and coordination responsibilities for the good functioning of SINS, composed of representatives of the competent authority, at state secretary level, or deputy state secretary. The CCS is chaired by the minister of administration and interior.

(4) The Technical Committee is established, hereinafter TC, coordinated by the Ministry of Administration and Interior, as a body with attributes of analysis and solving for technical problems that might appear in the functioning of NISA, composed by expert level representatives of all competent authorities, stipulated in the annex that is a part of the present emergency ordinance.

(5) The organization, functioning, organizational chart and attributes of the structures stipulated in Para (3) and (4) are established by the application norms of the present emergency ordinance.

Art. 4

(1) The ministry of Administration and Interior and competent authorities are obliged to adopt security measures for the management and use of NISA, aiming at:

a) The control of the access to equipment in order to block access of unauthorized persons to equipment working with personal data.

b) The control of data support in order to avoid unauthorized reading, copying, modifying or deleting of data support.

c) The control of stocking in order to avoid the unauthorized introduction of data and the unauthorized inspection, modifying or deleting of personal data.

d) The control of use, in order to avoid the use of automatic data processing systems by unauthorized persons helped by data transmission equipments.

e) Data access control, in order to limit access of authorized persons to the use of data automatic processing system only to data they have been authorized to.

f) Control of communications, in order to insure the checking and establishment of bodies that may be transmitted personal data using communication equipment.
g) The control of data introduction in order to ensure the possibility to subsequently check and establish what personal data were introduced into the automatic processing system, when and for who the data were introduced.
h) The control of data transport in order to avoid unauthorized reading, copying, modifying or deleting of personal data during the transmission or transport of data support.

(2) The Ministry of Administration and Interior and competent authorities will adopt technical, operative and procedure measures, following the next principles:

a) Confidentiality: information is accessible only for authorized persons according to their competences.
b) Integrity: ensuring the precision and complete character of information and also of processing methods
c) Availability: ensuring the access to information in due time.
d) Identification and certification: all the users are properly identified, according to their competences, before any transaction.
e) Authorization: the participants to a transaction are authorized to access NISA data according to their competences

CHAPTER III

LEGAL FRAMEWORK OF THE DATA ENTERED INTO NISA

Art. 5

(1) Data entered into NISA are directly related to certain persons and/or goods, upon the criteria foreseen at art. 6 and 7, and are provided and/or consulted by the following institutions:

a) Romanian Police
b) Romanian Border Police
c) Romanian Gendarmerie
d) Authority for Aliens
e) Sirene Bureau, once it becomes operational
f) National Office for Refuges
g) National Inspectorate for People Record
h) General Directorate for Passport issuing
i) Directorate for Driving Licenses and Cars Registration
j) National Authority for Customs
k) Ministry for Foreign Affaires
l) Ministry of Justice.

(2) The way of providing and/or consulting the data contained by NISA by the institutions foreseen in paragraph (1) is regulated in the annex to this document.

Art.6

Data on persons entered into NISA are the followings:

a) data on persons wanted for purposes of extradition or delivery, in accordance to a valid European Arrest Warrant;
b) Data on aliens for whom an alert has been issued for the purpose of refusing entry;

c) Data on aliens for whom the deportation, refusal of entry or removal decision has been issued;
d) Data on persons that have been refused to leave country;
e) Data on missing persons or persons who, for their own protection or in order to prevent threats, need temporarily to be placed under police protection at the request of the competent authority or the competent judicial authority of the Party issuing the alert;
f) Data on witness, persons summoned to appear before the judicial authority in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation f liberty shall be entered, at the request of the competent judicial authorities, for the purposes of communicating their place of residence or domicile.

Art.7

Data on goods, introduced in the NISA, refer to that objects which may be used as material evidence or are sought for the purpose of seizure in criminal proceedings, as:

(a) motor vehicles with a cylinder capacity exceeding 50 cc which have been stolen, misappropriated or lost;
(b) documents on vehicles, stolen, misappropriated or lost;
(c) car plates stolen, misappropriated or lost;
(d) trailers and caravans with a unloading weight exceeding 750 kg which have been stolen, misappropriated or lost;
(e) firearms which have been stolen, misappropriated or lost;
(f) blank official documents which have been stolen, misappropriated or lost;
(g) issued identity papers (passports, identity cards, driving licenses, residence and/or work permits) which have been stolen, misappropriated or lost;
(h) banknotes or valuable titles stolen, misappropriated or lost;
(i) other identifiable objects stolen, misappropriated or lost.

Art. 8

Personal data introduced in the NISA is composed, at maximum, of the following elements:

(a) surnames and forenames, any aliases possibly entered separately;
(b) any specific objective physical characteristics not subject to change;
(c) date and place of birth;
(d) sex;
(e) nationality;
(f) whether the persons concerned are armed, violent, or fugitive;
(g) reason for alert;
(h) action to be taken.

Art.9

(1) The access and processing the data entered in the NISA which relate to them shall be exercised in accordance with the national law regulating the protection of personal data and to the Convention for the protection of individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ratified by Law 682/2001, amended afterwards, exclusively by the competent authorities established by law and under the conditions set up by it.

(2) The conditions regarding the access to the data foreseen at art. 6 and 7, and the data stocking periods in the NISA are established by application provisions to the present emergency ordinance.

(3) Data is processed exclusively to the scope for which it was introduced in the NISA.

(4) The National Authority for Processing Personal Data is the competent authority for supervising and control of the data contained by NISA, and for its proper management. Within its scope, the above-mentioned Authority has full access to the NISA data.

Art. 10

(1) The competent authority are responsible for the authenticity, level of emergency, actuality and legality of data introduced in the NISA

(2) Only the competent authority issuing the alert shall be authorized to modify, add to, correct or delete data, which it has entered, until the expiry period established by law.

(3) Any interested person or competent authority, different from the one that introduced the data, may alert the competent authority indicated in para (2) of the fact that certain data introduced in the NISA are not *de iure* and *de facto* authentic. The competent authority foreseen by para (2) has the obligation to verify the alert, and, when necessary, to modify, add, alliterate or delete the data without any delay.

Art. 11

(1) Under the law, any interested person can request MoAI for information regarding his/her personal data existing in NISA.

(2) Under the law, any prejudiced person can request for the legal redress of the prejudice caused by introducing or exploiting his/her personal data in NISA.

CHAPTER IV
FINAL PROVISIONS

Art. 12

Current and capital expenditures for creating the system's technical support and NISA activity are ensured under the law, from the state budget through the MoAI's budget.

Art. 13

The NISA development is achieved on the basis of an implementation action plan approved by Government 6 month from the date of the entering into force of this Government emergency ordinance.

Art. 14

The norms for implementing this Government emergency ordinance are approved by Government decision in 1 year from the date of entering into force of this Government emergency ordinance.

Art. 15

The Annex to this Government Emergency Ordinance can be amended by Government decision, in accordance with the modifications of the competent authorities' legal attributions, as well as the categories of alerts managed by SIS.

Competent authorities in issuing and/or consult the alerts introduced in the SINS, upon data categories

No.	**CCompetent authorities** / **Description/reasons for alerts**	Romanian Police		Romanian Border Police		Romanian Gendarmerie		Authority for Aliens		SIRENE Bureau		National Office for Refugees		National Inspectorate for People Record		General Directorate for Passports		Directorate for Driving Licenses and Cars Registration		National Authority for Customs		Ministry of Foreign Affairs		Ministry of Justice	
		1		**2**		**3**		**4**		**5**		**6**		**7**		**8**		**9**		**10**		**11**		**12**	
		I	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**	**I**	**C**
1	Data on persons wanted for purposes of extradition or delivery, in accordance to a valid European Arrest Warrant		x		x		x		x	x	x		x												x
2	Data on aliens for whom an alert has been issued for the purpose of refusing entry		x	x	x		x	x	x		x		x										x		
3	Data on aliens for whom the deportation, refusal of entry or removal decision has been issued		x		x		x	x	x		x		x												
4	Data on persons that have been refused to leave country		x	x	x		x	x	x		x														
5	Data on missing persons or persons who, for their own protection or in	x	x		x		x				x														

RESTREINT UE

	order to prevent threats, need temporarily to be placed under police protection at the request of the competent authority or the competent judicial authority of the Party issuing the alert																								
6	Data on witness, persons summoned to appear before the judicial authority in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation f liberty shall be entered, at the request of the competent judicial authorities, for the purposes of communicating their place of residence or domicile	**x**	**x**		**x**		**x**	**x**	**x**		**x**		**x**												**x**
7	a) motor vehicles with a cylinder capacity exceeding 50 cc which have been stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**								**x**		**x**				
	b) documents on vehicles, stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**								**x**		**x**				
	c) car plates stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**								**x**		**x**				
	d) trailers and caravans with a unlading weight exceeding 750 kg which have been stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**								**x**		**x**				
	e) firearms which have been stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**										**x**				
	f) blank official documents which have been stolen, misappropriated or lost;	**x**	**x**		**x**		**x**		**x**		**x**		**x**		**x**		**x**		**x**		**x**				
	g) issued identity papers (passports, identity cards, driving licenses, residence and/or work permits) which have been stolen, misappropriated or lost;	**x**	**x**		**x**		**x**				**x**		**x**		**x**		**x**		**x**		**x**				
	h) banknotes or valuable titles stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**										**x**				
	i) other identifiable objects stolen, misappropriated or lost	**x**	**x**		**x**		**x**				**x**										**x**				

Note: I-issuing of data; C-consultation of data

ANNEX IV

Decision no. 1411 of October 11, 2006 on approving the Implementation rules of Government Emergency Ordinance no. 128/2005 on creating, organization and functioning of the National IT System for Alerts

CHAPTER I
AUTHORITIES WITH COMPETENCIES IN MANAGING AND USING THE NATIONAL IT SYSTEM FOR ALERTS

Article 1

(1) The Committee for Strategic Coordination, hereinafter called CSC, created according to the provisions of article 3 paragraph (3) of the Government Emergency Ordinance no. 128/2005 on creating, organization and functioning of the National IT System for Alerts, approved with amendments and additions by Law no. 345/2005, hereinafter called the emergency ordinance, for the purpose of analyzing and coordinating the functioning of the National IT System for Alerts, hereinafter called NISA, is a consulting body without legal status functioning by the Ministry of Administration and Interior.

(2) CSC is an inter-ministerial body chaired by the minister of administration and interior and made up of representatives, at the level of secretary of state or if case be, subsecretary of state, of the following public authorities:
   a) the Ministry of Administration and Interior;
   b) the Ministry of Justice;
   c) the Ministry of Foreign Affairs,
   d) the National Customs Authority.

(3) CSC has the role of facilitating and making efficient the communication and collaboration among the competent authorities, as well as substantiating the orders or if case be, the decisions of CSC regarding the taken measures and correlated actions concerning the creation, development and functioning of NISA.

Article 2

(1) CSC carries out its activity during bi-annual meetings or any time necessary, at the request of the CSC chairman.

(2) The CSC secretary sets the agenda of the day and presents the report concerning NISA implementation.

(3) The decisions of the CSC are recommendations, which may be the basis for proposals of normative acts and for measures taken by the heads of competent authorities.

(4) The financial resources necessary for the CSC meetings and CSC secretariat are supplied from the budget of the Ministry of Administration and Interior.

Article 3

(1) CSC has the main attributions:

a) it evaluates the degree of harmonization of the Romanian legislation with the Schengen acquis and drafts by its adopted decisions recommendations to the concerned institutions regarding the legal framework in order to bring it in line with the community and international practices or legislation;
b) it makes recommendations on earmarking funds for implementing and ensuring the NISA functioning;
c) it drafts, prepares and contributes to substantiating the decisions in order to ensure the coherence in the process of drafting and implementing strategies, policies and programs at the level of the competent authorities which provide and/or access alerts;
d) it analyzes the necessity and opportunity of including new authorities into the category of those mentioned in article 2 letter b of the emergency ordinance;
e) it analyzes the necessity and opportunity of including in the NISA new categories of alerts, as they are defined in article 2 letter a of the emergency ordinance and proposes the information they have to contain these categories of alerts;
f) f) it establishes if the institutions asking to become competent authorities have implemented the necessary measures for providing and/or accessing alerts;
g) it sets up working groups necessary for the development of the NISA;
h) it sets the manner of institutional cooperation in order to develop and render functional the NISA;
i) it drafts recommendations on eliminating the overlaps of competencies in NISA use among the competent authorities, by proposing the necessary measures;
j) it evaluates the fulfillment of the objectives mentioned in the Implementation Plan of the NISA;
k) it mediates the conflicts among the competent authorities which provided alerts according to article 8 paragraph 3.

(2) The president of the CSC may request the competent authorities ex officio or at the proposal of the Secretariat of the Strategic Coordination Committee, hereinafter called SCSC reports on the status of application of the Implementation Plan of the NISA, as well as reports on proposals on adopting necessary measures and presents annually to the Government a report on implementing and functioning of the NISA.

Article 4

(1) SCSC is headed by the General Directorate for European Affairs and International Relations of the Ministry of Administration and Interior.

(2) The position of secretary of the CSC is ensured by the director general of the General Directorate for European Affairs and International Relations.

(3) SCSC has the following main attributions:

a) it supervises the legislative and institutional amendments at the level of the European Union in the field of the Schengen Information System and it presents reports to the CSC;
b) it ensures the accurate dissemination to the competent authorities of the decisions taken within the working groups at the level of the European Union;
c) it ensures the permanent connection among the institutions represented in the CSC;
d) it drafts and presents to the CSC documents on the NISA put together on the basis of the data obtained from the competent authorities, as well as from other sources;
e) it supervises and communicates to the CSC the fulfillment of the duties and the status of implementing the specific activities for every competent authority, according to the Implementation Plan of the NISA;
f) it handles the documents of the CSC.

(4) The internal regulations of the SCSC is set by order of the minister of administration and interior.

Article 5

(1) The Technical Committee, hereinafter named TC is made up of representatives at the level of experts, of every competent authority mentioned in article 5 paragraph 1 of the emergency ordinance.

(2) The president of TC is the head of the central unit of the Ministry of Administration and Interior, which has attributions in the field of IT&C.

(3) TC has the following main attributions:
a) it analyzes the modernization of the IT&C systems which participate in the NISA in order to render them compatible with the NISA;
b) it analyzes the technical problems notified by the competent authorities as they arise during the implementation and functioning of the NISA and proposes solutions to the CSC;
c) it ensures the implementation of the decisions of the CSC from a technical point of view;
d) it presents to the SCSC proposals for a better functioning of the NISA and the proposals are forwarded through the CSC;
e) it ensures the competent authorities reports regarding the decisions taken in the technical working groups of the European Union in the field of the Schengen Information System;

(4) TC meets once a trimester or as necessary at the request of the committee president.

(5) The Secretariat of the TC is ensured by the central structure of the Ministry of Administration and Interior, which has attributions in the field of IT&C.

(6) The Secretariat of the TC has the following main attributions:
a) it supervises the technical changes at the level of the European Union in the field of the Schengen Information System and sends reports to the TC and SCSC and presents to the CSC;
b) it ensures the permanent connection among the authorities represented in the TC;

c) it drafts and sends to the SCSC in order to be presented in the CSC documents on the technical issues of the NISA made up on the basis of the data obtained from the competent authorities, as well as from other sources;

d) it handles the documents of the TC.

CHAPTER II
THE ACCESS AND STORING OF THE DATA IN THE NISA

Article 6

(1) The competent authorities access only the alerts of the NISA necessary for fulfilling their own attributions and ensure access to them only for duly authorized personnel.

(2) The alerts in the NISA cannot be transferred, downloaded or copied, except for the cases mentioned in article 4 paragraph 3 of the emergency ordinance.

(3) Every providing and/or accessing of personal data shall be recorded in the NISA for the purpose of checking the admissibility of the providing and/or search. The record may be used only for that purpose and shall be deleted at the earliest after one year and at the latest after three years.

(4) In the purpose providing and/or accessing the alerts in the NISA, the competent authorities shall issue a common methodology with technical, operative and procedural measures correlated with the security requirements issued by the national authorities.

Article 7

(1) The competent authority, which provided the alert, is authorized to amend, supplement or delete the data, which it entered.

(2) If one of the competent authorities which did not issue an alert has evidence to prove that a piece of data is false, inaccurate or was stored illegally, it shall inform in 10 days the competent authority that provided the alert about this.

(3) The competent authority which entered the alert has the obligation to check the evidence mentioned in paragraph 2 and if it is necessary, to modify or delete immediately the respective data.

(4) In case an understanding cannot be reached, the competent authority, which did not enter the alert, shall forward the case for mediation to the CSC.

Article 8

(1) Before entering an alert on a person, the competent authority must check if that person is the subject of another alert previously entered into the NISA.

(2) If following the checks, it is established that a person with the same identification data is subject of a previous alert, the competent authority which wants to enter the new alert shall contact the competent authority which firstly entered that alert in order to established if it concerns the same person.

(3) If following the consultations, it is established that the previous alert concerns the same person, the new data provided by the latest competent authority in the NISA is automatically added to the already existing NISA alert.

(4) In the case of persons for whom different measures were requested by several competent authorities, the competent authority that identifies the person shall inform all the other competent authorities that requested measures to be taken about it. The order in which the measures will be taken shall be established by the competent authority, which identifies the person.

Article 9

(1) The personal data entered into NISA according to the provisions of article 6 of the emergency ordinance are stored only for the time necessary to achieve the purpose for which they were entered.

(2) Before the expiry of the three years period from the time of NISA entering, the providing competent authority analyzes the necessity of preserving it into the system. The alert can be preserved if it is necessary for achieving the purpose for which it was entered in the NISA.

(3) Any extension of the validity period of an alert is communicated to the central unit of the Ministry of Administration and Interior, which manages the NISA from a technical point of view according to article 3 paragraph 2 of the emergency ordinance.

(4) The maximum storing time for the data mentioned in article 6 letters d to f of the emergency ordinance is of 10 years.

(5) The maximum storing time for the data mentioned in article 7 of the emergency ordinance is of 5 years.

(6) The maximum storing time for the data mentioned in article 6 letter a to c of the emergency ordinance is set by the competent authority, depending on the case.

(7) The technical support function of the NISA informs automatically the competent authorities that entered the alerts on their planned deletion from the system a month in advance before the completion of the maximum storing period.

(8) The deleted alerts are kept for one year in the system in order to be accessed for checking the accuracy and legality for them being entered and afterward, they are destroyed.