THE NATIONAL SUPERVISORY AUTHORITY
FOR PERSONAL DATA PROCESSING

ANNUAL REPORT

2016

The activity report is presented to the Romanian Senate, according to Article 5 of Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing, with further changes and amendments.

Bucharest

FOREWORD

Mr. President of the Senate,

Dear Senators,

2016 marks the begining of a major reform on the data protection field at national lever, as a direct effect of the adoption on the 27th of April 2016 by the European Parliament and Council of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as of Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The direct applicability of the General Data Protection Regulation starting with the 25th of May 2018 will result in harmonizing the principles of data protection in all Member States of the European Union, by replacing the existing national regulations.

With reference to this new European regulation, we note a strengthening of the rights of individuals by either by developing the existing ones or by establishing new rights such as the right to be forgotter, the right to data portability and the right to restriction of processing. In the same time, the responsibility of the data controller in relation to the processing performed by them was emphasized.

Another element of novelty introduced by the Regulation for which I would like to draw your attention is the obligation of the public institutions and, in certain cases, of the private entities to designate internally a data protection officer, according to certain criteria.

We underline that this will involve a significant change in the activity of data controllers in Romania, designed to make the data controllers accountable, and we hope that wit will have beneficial effects in terms of respecting the data subjects' rights.

Under the conditions in which the General Data Protection Regulation contains some provisions which allow Member States to intervene adjacent with certain national legislation, during 2016 the consultations with the ministries responsible for analyzing and preparing the appropriate national framework were initiated.

As the General Data Protection Regulation provides for an extension of the competences and tasks of the national supervisory authorities, there is need for certain amendments of the national legislation that would strengthen the institutional and administrative capacity of the national supervisory Authority, including the allocation and provision of appropriate human, material and financial resources.

Since next year will be crucial in ensuring the proper implementation of these new regulations, we propose that the actions of the Authority to be subsumed under the following main objectives:

- the active involvement in preparing the national legal framework in line with the new EU regulations, together with the responsible institutions;
- increasing the awareness amond the data controllers and citizents on the application of the new rules, with the support of mass-media' and civil society's representatives.

In this context, the strengthen of the administrative capacity of the Authority for fulfilling the new tasks established on an adequate level represents a priority and implies the allocation of material, financial and human resources in order to ensure a real protection of the right to privacy and to protection of personal data, at European standards.

Finally, please allow me to express my hope that the Authority will benefit also in the future from your support in this important time of reform in the data protection field.

Ancuţa Gianina OPRE,

President

TABLE OF CONTENTS

CHAPTER I

OVERVIEW

The activity report of the National Supervisory Authority for Personal Data Processing (hereafter the national supervisory Authority) for 2016 is structured in 7 chapters, as follows:

Chapter I provides an overview summary report on the main issues.

In **Chapter II** the relevant issues on the legislative package reform in the data protection field, adopted on 27th of April 2016 at EU level, in particular with regard to the applicability of the General Data Protection Regulation in all Member States starting with the 25th of May 2018 are presented.

Chapter III contains relevant information on the advisory activity for proposals for normative acts and on the consulation activity on the application of data protection rules, including the clarification of certain issues raised by different data controllers. This resulted in issuing opinions on a number almost double of proposals for normative acts and on a significant number of opinions in general.

The natural persons and the data controllers requested, mainly, information on the conditions for processing personal data, including sensitive data, as well as information referring to the legality for the disclosure of certain data.

In the section on the representation before courts of law, the most significant cases litigations to which the National Supervisory Authority for Personal Data Processing was a part of and the given resolutions are underlined.

The section on the public information shows the main methods of popularising the personal data protection field, used during 2016, within the limits of the allocated budgetary resources.

Chapter IV consists of a presentation of the control activity, concerning the ex officio investigations and those carried out based on the complaints or notices received, which implies the verification of the applicationf of the legal provisions in this field. In order to intensify the investigations carried out during 2016, fines were applied with a total of over 1 million lei.

The ex officio investigations focused on the compliance of the data controllers from different sectors of activity with the provisions of Law no. 677/2001, as well as of other legislative acts concerning the personal data field.

In some cases, by decision of the president of the national supervisory Authority, it was decided to end processing operations or to delete the processed data.

Chapter V presents the foreign affairs' activity of the national supervisory Authority.

Chapter VI on personal data processing supervisory activity shows the conclusions drawn from analyzing the forms sent by the data controllers, natural and legal persons that had the obligations to send them. A total of 6930 notifications about data processing have been registered, taking into consideration that the administrative burden of the data controllers was reduced by the application of Decision no. 200/2015 of the national supervisory Authority.

Chapter VII on the material and financial resources contains information about the budgetary credits available for the national supervisory Authority and the sums spent on every article of the budgetary classification.

CHAPTER II
NEW EUROPEAN UNION LEGISLATIVE ACTS

Section 1: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as well as of Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

The legislative package adopted on the 27th of April 2016 contains 2 normative acts:

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- Directive (EU) 2016/680 on the protection of data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences and other judiciary activities.

Regarding the nature of the legal instrument, the European Commission proposed a regulation, a normative act with a direct applicability, with the declared intention to ensure a regulatory unit and approach in the data protection field at EU level.

The adoption of the General Data Protection Regulation constitutes an important moment in the personal data protection field, with direct effect on the activity of the data controllers, bearing in mind that the specific rights of the natural persons are consolidated.

Thus, we note a consolidation of the right to erasure, by explicitely enshirining the "right to be forgotten", and on the other side it establishes the right to data portability and the right to restriction of processing, in order to give citizens a better control of their personal data.

An element of novelty introduced by the Regulation is the obligation of the public institutions and of the private entities to designate internally a data protection officer, according to certain criteria.

This will involve a significant change in the activity of the data controllers from Romania as will suppose the elimination of the existing data processing notification declared at the national supervisory Authority.

In the same time, it was achieved a more detailed regulation on the obligation of the data controllers, with a particular emphasis on the increase of their accountability.

The express consecration of the priciples of privacy by design and privacy by default represents another novelty of this regulation, implying the ensurance of the protection of data from the initial moment of establishing the processing means.

At the same time, we underline that the Regulation contains certain dispositions which offer the Member States the possibility to intervene with certain national regulations.

A new mechanism for the cooperation between the data protection authorities is forseen, which involves a European body with legal personality – the European Data Protection Board (EDPB). It will be responsible for the mediation of disputes between the data protection authorities, as well as for the drawing up guidelines and recommendations for establishing a unitary application of this new regulation within the EU.

It provides an extension of the competences and tasks of the national supervisory authorities and, as a consequence, there is a need for certain amendments of the national legislation that would strengthen the institutional and administrative capacity of the national supervisory Authority, including the allocation and provision of appropriate human, material and financial resources.

The provisions of the General Data Protection Regulation will apply starting with the 25th of May 2018.

CHAPTER III
REGULATORY ACTIVITY, ADVISING, CONSULTATION AND PUBLIC INFORMATION

Section 1 Approval of legislative acts

According to Article 21 (3) h) of Law no. 677/2001, the national supervisory Authority issued opinions on 56 legislative proposals elaborated by various institutions and public authorities, which referred to aspects concerning personal data processing

Given the increasing number of normative acts submitted for approval, in most cases it was considered necessary to amend those texts, observations and proposals in relation to the need to respect the principles and conditions for the processing of personal data were made.

Recommendations for the re-examination of the texts and their harmonization with the laws on data protection were issued on most of the legislative proposals.

Some of the relevant legislative proposals analyzed are detailed below as an example:

- **National Authority for Consumer Protection sumitted for approval the proposal for "Ordinance on cred agreements for consumers for real estate"**

The following observations and proposals were issued:

Regarding the provisions of Article 9 (2) a) of Chapter III, corroborated with the ones of Chapter XIII "creditworthiness assessment" of the proposal, it was underlined that, within the context of personal data processing, the data controllers have the obligation to inform the data subjects, according to Article 12 (1) of Law no. 677/2001 corroborated with the provisions of Decision no. 105/2007 regarding the processing of personal data performed in an evidence system of credit bureau type systems.

Compared to Article 21 (1) of the proposal, it was considered necessary to correlate its provisions with the ones of Law no. 677/2001, according to which when exercising the right of access to data, the right of intervention and the right to oppose, the data controllers have the obligation to give an answer within 15 days of receipt of the request.

It was also assessed as being appropriate to re-examine the provision of Article 27 (1) o) of the proposal referring to consumers' information with reference to the specific effects the proposed products may have on them, including the consequences in the event of unpayment by the consumer, taking into account the provisions of Article 12 of Law no. 677/2001, corroborated with the provisions of Decision no. 105/2007, as well as the legale provisions regarding the Central Credit Risk.

With reference to Chapter XII of the proposal "assessing the creditworthness of consumers", it was highlighted that the provisions do not adequately transpose Article 18 (5) c) of Directive 2014/17/EU and, as consequence, it was considered as necessary its reformulation.

As regards Article 73 (1) of the proposal, it was assessed as necessary to amend it by taking into consideration the dispositions of Article 4 (1) e) of Law no. 677/2001 which provide that the personal data which are intended to be processed must be 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.

Referring to Article 74 (1) of the proposal, it was pointed out that "the consumers' income and expenses levels" and the "financial and economic information" of the credit applicants are personal data whose processing is subject to conditions established by Law no. 677/2001.

Regarding the dispositions of Article 74 (3) of the proposals on the "obtaining" the previous-mentioned information by the creditors also from "relevant internal or external sources, it was considered to be necessary to supplement them in order to include the mention that the information necessary for the assessement of the consumers' creditworthness should be necessary, sufficient and proportionale in accordance with Article 20 (1) of Directive 2014/17/EU.

On Article 78 of the proposal, it was underlined that, with reference to the processing of personal data of the consumers natural persons in order to assess their creditworthness, the observance of Law no. 677/2001 implies, along with taking into consideration the data protection principles, also respecting all the data subjects' rights, establishing the persons, respectively the authorised entities (according to provisions of Article 79 of the proposal) which will have access to data for legitimate purposes, as well as ensuring the confidentiality and security of the personal data processing.

Bearing in mind the provisions from the proposal referring to the "access to the database" it was stated that, in connection to the electronic communication of data between different entities mentioned in the legislative proposal, such a communication can be exposed to a series of risks such as loss, destruction of data etc., even accidental. Or, when establishing the means of transmission of data or documents that contain personal data, it should be taken into consideration that the data controllers have the obligation to adopt appropriate technical and organisational measures in order to protect the personal data against the accidental or illegal distruction, loss, alteration, dissemination or unauthorised access, notably if the respective processing involves the data transmission within a network, as well as against any other form of illegal processing, having regard to Article 17 (1) of Directive 95/46/EC of European Parliament and provisions of Article 20 of Law no. 677/2001.

In the context of dispositions of Article 104 (3) of the proposal, it was proposed its reformulation by taking into consideration that, according to Article 20 (5) of Law no. 677/2001, the processing by data processors should be carried out based on a contract concluded in a written form, which shall necessarily contain the obligation of the data processor to act strictly in accordance with the instruction received from the data controller and the fact that accomplishing the obligations concerning the security measures also apply to the data processor.

As a consequece, the national supervisory Authority **approved with observations** the proposal for "Ordinance on cred agreements for consumers for real estate".

- **National Gambling Office submitted a request for the opinion on the proposal for a Decision for the approval of the Methodological norms for the application of Emergency Ordinance no. 77/2009 on the organization and use of gambling and for the modification and supplementation of Government Decision no. 298/2013 on the organization and functioning of the National Gambling Office and for the modification of Government Decision no. 870/2009 for the approval of the Methodological norms for the application of Government Emergency Ordinance no. 77/2009, with further changes and amendments on the organisation and use of gambling**

With reference to this proposal, the national supervisory Authority issued the following observations and proposals:

The activities that are going to be carried out within the evidence systems of the entities involved in the organization and use of gambling involve the processing of personal data of individuals (including sensitive data such as the personal identification number, the series and number of the identity card or other information within the documents which prove the identity of the persons).

As such, it was considered necessary to take into account the data protection principles stated by Article 4 (1) of Law no. 677/2001, since the creation of records in an automated form, whereas the activity of organization and use of gambling takes place within certain systems.

It was also considered necessary to give more attention to the implementation of adequate safeguards for the observance of the rights of data subjects and for the identification of the responsibilities and means of access to data for all the entities involved, based on legal competences, as well as for the clarification of their quality, namely data controller or data processors, within the terms of Law no. 677/2001.

Thus, it was recommended to establish a complete list of the data collected in order to avoid the infringement of the principle stated in Article 4 (1) c) of Law no. 677/2001.

It was found it necessary to clearly establish the data and categories of data collected and processed by the authorised authorities in order to provide predictability and foreseeablity.

With reference to the principle stated in Article 4 (1) e) of Law no. 677/2001, it was considered necessary to establish an accurate retention period, according to the duration necessary to achieve the purposes.

Also, it was found it necessary to identify and to expressively mention the quality of data controller or data processor, depending on the case, of each entity that collects and processes personal data, and inserting statements in the text of the proposal on the fact that they are required to ensure compliance with the provisions of Law no. 677/2001 and Law no. 506/2004, especially with reference to the rights of data subjects and confidentiality and security.

Meanwhile, in terms of informing the data subjects, it was pointed out that this is an obligation incumbent on all entities engaged in the organization and use of gambling.

With reference to the obligations mentioned above, it was recommended either the insertion of a separate article, or the insertion of statements within the articles which refers to the activity data controller to collect and process data.

Taking into consideration the above, **the Authority considered that the proposal of decision should be subject to a review.**

- **The Ministry of Labour, Family, Social Protection and Elderly submitted for approval the proposal for a Law on minimum income inclusion**

With reference to this proposal, the national supervisory Authority issued the following observations and proposals:

Regarding Article 29 (1) of the proposal, as well as regarding the other articles which mention the electronic mean for communication of the requests for granting the minimum income inclusion, it was highlighted that this system may expose the communication to a series of risks.

On Article 29 (2) and (4) of the proposal, it was found that these dispositions, by using the term "mainly", do not present entire list of data and categories of data requested, which denotes ambiguity and may lead to the excessive collection of personal data, thus infringing the principle stated by Article 4 (1) c) of Law no. 677/2001, namely the adequate, relevant and nonexcessive character of the data.

Therefore, it was found it necessary to clearly establish the data and categories of data collected and processed by the authorised authorities in order to provide predictability and foreseeablity.

The same arguments were presented also with regard to the phrase „data on the righthful person" which does not clearly indicate the data strictly necessary for the accomplishment of the purpose (granting the minimum income) and which may also lead to unharmonized application of the law.

In this context, due to the fact that Article 29 (6) of the legislative proposal provides that methodological norms for the application of the law will be elaborated, it was recommended for these subsequent normative acts to include information about the means for collecting the data, observance of the principles stated by Article 4 of Law no. 677/2001 (the adequate character of the data and categories of data collection, updating the data, retention periods, conditions for the deletion of data), means for exercising the rights of the data subjects, in particular the right of access and that the data controller is obliged to apply measures for ensuring the confidentiality and security of data.

With regard to Article 32 of the legislative proposal, it was highlighted that the activities to be carried out by the entities involved in the activity of granting the minimum income within the evidence systems imply the processing of a large volume of personal data of individuals

(including sensitive data such as health data, personal identification number, series and number of the identity card etc.).

Thus, the implementation at national level of such an electronic system for the collection and processing of personal data of individuals applying for the minimum income of inclusion is likely to present special risks towards the rights and liberties of this category of persons. As a concequence, it is very important to ensure a real protection of personal data according to provisions of Law no. 677/2001, with further changes and amendments.

Thus, when proposing and designing automated filing systems, as one presented in the legislative proposal, it is necessary to take into consideration the data protection principles stated by Article 4 (1) of Law no. 677/2001, since the creation of records in automated form, namely the National Information System for Social Assistence.

In this context, it was deemed necessary to pay a special attention to establishing the appropriate safeguards for respecting the rights of the data subjects, as well as for identifying the responsibilities and means of access for all the entities involved, by taking into account their legal competences, as well as clarifying their quality of data controllers or data processors, as defined by Law no. 677/2001.

It was also considered to be useful to insert a new paragraph in Article 32 stating that the "collection and processing of data necessary to grant the minimum income of inclusion will be carried out by observing the provisions of Law no. 677/2001, in particular the rights of data subjects and the confidentiality and security of data".

It was considered to be necessary to introduce a new paragraph in Article 37 stating that "the employees of the local public administration shall observe the confidentiality and security of information and personal data according to dispositions of Law no. 677/2001".

In the same time, the wording of Article 38 (1) of the proposal, in connection to accessing "other available databases of other public authorities with which protocol of cooperation were concluded", is not clear, thus contravenes the principle referring to the adequate, relevant and not excessive character of data, infringing the principles of predictability and foreseeablity that must be complied with.

Moreover, the protocols of cooperation are known only by the signatory entities and less by the individuals concerned and, thus, the individuals are not aware of their data which are required, as well as of hte providing authority or institution.

It was stated that the Court of Justice of European had the same opinion as the one mentioned above in Case C-201/14 (Bara and other, preliminary request submitted by Curtea de Apel Cluj) on the legal basis for the transmission of personal data on personal income between ANAF and CNAS, as follows: „the detailed arrangements for transferring that information were laid down not in a legislative measure but in the 2007 Protocol agreed between the ANAF and the CNAS, which was not the subject of an official publication."

Moreover, the pharse „in the agreed electronic format" from paragraph (2) of the same article is not clear and, thus, may produce a nonharmonized application, reason for which is necessary to establish a concrete electronic format, as well as the means for the electronic transmission, in order to avoid the risk situations which were mentioned in Article 29 (1) of the proposal.

In light of the aboves, the Authority considered that the **proposal of Law on minimum income inclusion should be subject to a review**, in terms of the observations and proposals previously mentioned.

- **The Romanian Government requested proposals and observations concerning the legislative proposal for amending and supplementing Law no. 1/2011, updated version on the 01.10.2015, on national education (Plx 182/2016)**

The national supervisory Authority issued the following observations and proposals:

The processing of personal data by use of video surveillance systems is subject to Law no. 677/2001, as amended and supplemented, Decision no. 52/2012 on the processing of personal data through video surveillance means (published in the Official Journal no. 389 of the 11th of June 2012), Law no. 333/203 on the security of objectives, goods, valuables and the protection of individuals, as amended and supplemented and the Methodological norms approved by Government Decision no. 301/2012.

The legislative proposal regulates the restriction of some rights and liberties which should observe the conditions established by Article 53 of the Constitution, in particular to meet the requirement of necessity and proportionality of the measure which caused the situation.

Therefore, establishing by law, as necessary, a permanent monitoring by video surveillance of individuals, including minors, can be performed only if the measure is proportionate to the risks faced by the data controller (the school in question).

The explanatory memorandum does not refer to a possible legislative insufficiency in this domain so it should be necessary to adopt such a legal regulation. However, as noted above, there is currently a regulatory framework in force in this area.

In the same time, according to Article 13 of Law no. 24/2000, modified and amended, and taking into considerations the mentions from Section V of the Explanatory memorandum, we state that in the jurisprudence of the European Court of Human Rights with reference to Article 8 of Convention for the Protection of Human Rights and Fundamental (the right to respect for private and family life), the European court held that it is not always possible to make a clear distinction between the activities of individuals who are part of their professional life and those who fall out of this category (Case Niemietz v. Germany, December 16, 1992) and there is no reason not to allow the exclusion of professional or business nature from the notion of "private life" (Halford v. the United Kingdom, June 25, 1997), and that the protection offered by Article 8 should be reduced to unacceptable way if the use of modern scientific techniques is permissible at any cost and without striking a balance between the benefits of extensive use of these techniques and important interests related to privacy (Case S. and M. Marper v. the United Kingdom, December 4, 2008).

With reference to the legislative proposal, we consider that the current form to be in contradiction with the legal framework in force and that it creates a legislative parallelism.

Thus, Article 274 from the proposal refers erroneously to Directive no. 52/2012 which is in fact Decisio no. 52/2012, an administrative act with a normative character issued by the national supervisory Authority.

This decision was issued based on Law no. 677/2001 and on the competences of the national supervisory Authority established by Law no. 102/2005, by taking into consideration the requirements for a normative intervention such as the processing of personal data through the use of specific technical means – video surveillance systems, basic principles and the purpose of the proposed regulation, as well as the effects taken into account, with reference to the purpose of the regulations, namely ensuring an efficient protection of the rights and fundamental liberties of individuals, in particular the right to the protection of personal data where the processing is carried out through techniques of capturing, transmitting, handling, recording, storing or communicating the data from the images of natural persons which represents personal data processing operations.

Thus, Decision no. 52/2012 contains rules of principle (which are, moreover, provided also by Law no. 677/2001) for an indeterminate number of persons and contains not only legally binding rules (which require a certain activity, eg. information to data subjects), but also prohibitive ones (prohibiting a certain activity, for example, the image storage for a period exceeding 30 days) or permissive (which provides the possibility to perform a certain activity under specified conditions).

In consideration of the various hypotheses that may arise in its application, the text of the decision regulates also the video surveillance of employees, regardless of the industry, as well as children, regardless of where they are.

Thus, Article 3 corroborated with Article 6, Article 8 and Article 9 of Decision no. 52/2012 stipulates that the processing of personal data by the use of video surveillance is conducted in compliance with general rules laid down in Article 4 of Law no. 677/2001, as amended and supplemented, in particular the principle of proportionality and the data subject's consent or other exceptional conditions provided by law.

Article 8 of Decision no. 52/2012 establishes the situations when the processing of personal data of employees by means of video surveillance is permitted, namely: to fulfill the legal obligations under an express or legitimate interest, by observing the rights of the employees, in particular their prior information.

Paragraph (3) of the same article of Decision no. 52/2012 provides that "the processing of employees' personal data using video surveillance inside the offices where they carry out their duties at the work place is forbidden, except for the cases expressly provided for by the law or with the notice given by the National Supervisory Authority for Personal Data Processing."

Therefore, with reference to the employees (teachers, auxiliary staff), due to the fact that the implementation of such a video surveillance system may affect their rights as employees, the provisons of the Labour Code, as well as the Status of teachers must be respected, in addition to the ones of Law no. 677/2001, as amended and supplemented, and of Article 8 Decision no. 52/2012.

It was also stated that the national supervisory Authority has obtained final and irrevocable decisions in court in which it was held that the processing of personal data (images) of employees in offices was carried out illegaly because, prior to implementation of video surveillance devices, there was no thorough analisys on the necessity and proportionality of

such a measure and there were not identified alternatives that have less impact on the privacy of employees.

Additionally, the court established that by installing video surveillance cameras the right to privacy of employees was infringed and it was created a discomfort among the persons who were visualized.

With regard to students, Article 9 of Decision no. 52/2012 establishes that the processing of minors' personal data using video surveillance means, including their disclosure, is allowed only with the express consent given by the legal representative or under the conditions provided by Article 5(2) of Law. no 677/2001, with the subsequent modifications and amendments, whilst observing their rights, especially that of prior information.

These provisions are corroborated with the ones of Article 27 of Law no. 272/2004 on the protection and promotion of the rights of the child, republished, which quarantee the right to have his or her public image and personal, private and family life protected, and any action which may affect the public image of the child or the child's right to personal, private and family life is forbidden.

According to the same law (Article 24), the child child who has the capacity to discern has the right to freely express his or her opinion regarding any matter which involves him or her, as well as the right to be heard in any judicial or administrative procedure which involves him or her.

In this context, we emphasize that the right to privacy of students, as well as of teachers and other school employees, but also the essential freedom of the didactic (freedom of students to learn and speak, freedom of teaching) should be considered a priority need for the constant surveillance by video means.

Related to the issues mentioned above, it was stated that, based on the provisions of Article 8 (3) of Decision No. 52/2012, the national supervisory Authority received requests from schools for approving the implementation of video surveillance systems in some offices, chancelleries and in classrooms (during the entire year), by considering these areas to be inside offices where teachers and other staff work.

With reference to the request of carrying out video surveillance in classrooms in other periods that the ones when the national examinations take place, as well as the video surveillance in offices and chancelleries, the national supervisory Authority did not approve the installation the video surveillance systems, taking account several aspects, such as: the schools

applying for approval have not presented justified arguments on the legitimate interest of the installation of such a surveillance system so that it prevail over fundamental rights and freedoms or the interests of individuals surveilled by using this system; there was no proof that nor the consultation of trade union or employees' representatives was carried out, neither the expressed and unequivocal consent of all employees and legal representatives minors was obtained; nor the explicit purpose was not indicated, neither the necessity of the personal data processing o the individuals carrying out their activity in the classrooms, in offices or chancelleries through video surveillance systems was sufficiently justified.

In light of the above and taking into account the need to ensure an effective protection of the fundamental right to privacy of individuals supervised by use of video surveillance, the national supervisory Authority considered that the requested approval may be granted in exceptional cases only by observing all the conditions listed above and only in justified and documented situations.

In this context, our institution transmitted its opinion to the Ministry of Education and Scientific Research, with the recommendation to communicate the opinion to school inspectorates and to all school units in order for their requests of approval to meet the legal requirements mentioned previously.

Coming back to the legislative proposal, regarding Article 276 (1) of the proposal, where it is mentioned the storage of the records for 90 days, this retention period is in contradiction the provisions of Article 14 of Decision no. 52/2012, which establish a period which should not be longer than 30 days, as well as with the provisions of Law no. 333/2003 and its methodological norms, which provide a period of 20 days, thus being excessive in relation with the purpose of the data processing.

In the same time, the legislative proposal does not provide, in the same article, archiving periods for the records, as well as the obligation to destroy or delete, depending on the case, in order to observe the principle stated by Article 4 (1) e) of Law no. 677/2001 and in accordance with the dispositions of Article 14 of the decision mentioned above.

Moreover, with reference to the conditions for exercising the right of access for paragraphs (2) and (3) of the same Article 276, as well as the ones for disclosuring the records, established in Article 278, they are in contradiction with the conditions stipulated by Article 13 of Law no. 677/2001 and, in the same time, affect the right to oppose and the right of intervention from the same law (Articles 14 and 15).

Also, Article 277 of the legislative proposal contravines the legitimacy requirements of the data processing without the consent of the data subject provided by Article 5 (2) of Law no. 677/2001.

On Article 280 of the legislative proposal, we noted that it regulates the access of the parents to the recorded video footage.

In this context, it was pointerd out that, when choosing the means for processing personal data, it should be borne in mind that entities holding data and the ones which come into possession of data have the obligation to maintain the confidentiality of the data processed and to apply appropriate technical and organisation measures in order to protect personal data, according to Article 19 and 20 of Law no. 677/2001.

In view of the above, it was underlined that such transmission of records may rise some risks for data protection of individuals (in this case, especially minors) and thus to the respect and guarantee of fundamental rights thereof, especially to intimate, family and private life. In this sense, the possibility of interception of images transmitted over the Internet in real time, due to current advanced information technologies, leads to viewing them by an indefinite number of people with potential further use which is not in accordance with the legal provisions on data protection and with the risk of serious prejudice to the rights and freedoms of individuals.

As a consequence, in light of the observations presented previously, taking into account the necessity of observing the requirements of Article 53 of the Constitution, in view of the provisions of Law no. 24/2000, modified and amended, as well as the existence of the legal framework in this domain, the national supervisory Authority **did not support the text of the legislative proposal** on the modification and amendment of Law no. 1/2011, updated version on the 2nd of October 2015 on national education (Plx 182/2016).

- **The Romanian Government submitted the legislative proposal for amending Article 5 of Law no. 677/2001 (Bp 181/2016)**

With reference to this proposal, the national supervisory Authority presented the following observations:

Law no. 677/2001 implemented in Romania Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 95/46/EC intends, as noted in particular in Recital (8), for the level of protection of the rights and freedoms of individuals with regard to the processing of such data to be equivalent in all Member States. In Recital (10) of this directive it is added that the approximation of national laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

Thus, the provisions of Article 7 of Directive 95/46/EC entitles "Criteria for making data processing legitimate" were implemented by Article 5 of Law no. 677/2001.

In this context, we state that, according to Article 5 of Chapter II of Directive 65/46/EC entitled "General rules on the lawfulness of the processing of personal data", the Member States list, within the limits of the provisions of the current chapter, the conditions in which the personal data processing is lawful.

Thus, this article allows the Member State only to mention, within the limis of Chapter II of the above mentioned directive and, therefore, of Article 7, the conditions in which the personal data processing is lawful.

It results that Member States may neither add new principles on the legitimacy of personal data processing than those provided for in Article 7 of Directive 65/46/CE nor to provide additional requirements to modify the contents of one of the 6 principles set out in this article.

Therefore, the discretion of Member States under Article 5 can be used only in accordance with the purpose of Directive 95/46/EC, which is to maintain a balance between free movement of personal data and the protection of privacy.

As a consequence, pursuant to Article 5 of Directive 95/46/EC, Member States can neither introduce other principles regarding the legitimacy of the processing of personal data than those provided for in Article 7 of the Directive nor to amend, by additional requirements, the content of the six principles mentioned in Article 7.

This interpretation is confirmed by the phrase "to be processed only if" and by conjuction "or" from the text of Article 7 of Directive 95/46/EC which highlight the exhaustive and limitative nature of the list provided by this article.

The Court of Justice of European Union ruled in line with the above in joined Cases C-468/10 and C-469/10.

In this context, we underline that the proposal for complementing the conditions of Article 5 of Law no. 677/2001 adds an additional condition which is not in the principles related

to legitimate processing operations under Article 7 of Directive 95/46/EC and imposes, without the consent of the data subject, the disclosure of his/her data, resulting in an lessening of the protection this Directive it offering.

Therefore, the proposal is not compatible with Directive 95/46/EC and is contrary to EUCJ jurisprudence.

Consequently, the national supervisory Authority **expressed that this legislative proposal law should be dismissed**.

- **The National Agency for Fiscal Administration submitted a request for proposals ans observations with reference to the proposal for Order for the modification and supplementation of the Procedure for publishing the lists of the debtors who register outstanding tax obligations, as well as their amount, approved by Order of the president of the National Agency for Fiscal Administration no. 558/2016**

With reference to the proposal of Order, the following were stated:

When publishing on its own website the List of the debtors – natural persons who register outstanding tax obligation to general consolidated budget, as well as the amount of these obligations (Annex no. 2 to the procedure approved by the proposal order under consideration), the National Agency for Fiscal Administration, as data controller, shall carry out the processing of data, by observing the general rules provided by Law no. 677/2001.

It drew attention to the provisions of points 11, 13, 14, 15, 16 of the Procedure approved by the proposal order under consideration and stressed that the data controller the National Agency for Fiscal Administration has the overall responsibility for ensuring accuracy and updating of personal data disclosed by disclosing the list comprising debtors natural persons, outstanding tax obligations to the general consolidated budget and the amount of their obligations.

The National Agency for Fiscal Administration has the obligation to respect the right to information of data subjects, as aprovided by Article 12, to respect the rights of the natural persons whose data are processed, as provided by Articles 13-18, as well as the obligation to ensure the confidentiality and security of the data processing, as provided by Articles 19 and 20.

On the necessity to ensure full information of the debtors, according to Article 12 of Law no. 677/2001, it was emphasized that it is necessary for the National Agency for Fiscal Administration to take into consideration the dispositions of the Court of Justice of European union in its decision in Case Smaranda Bara and others (C-201/14), even for the disclosure of personal data through the publishing of the Debtors List – natural persons who register outstanding tax obligations to the general consolidated budget, as well as the amount of these obligations.

As a result of applying the principles of data processing provided by Article 4 of Law no. 677/2001, is was proposed the modification of pct. 3 and 5 of the procedure approved from the proposal for Order, so as not to be considered outstanding tax obligations the disputed tax obligations until a final judgement is reached and, thus, not to publish their amount. Therefore, we proposed the removal of the fields "disputed tax liabilities" from the list of debtors – natural persons who register outstanding tax obligations to the general consolidated budget and the amount of these obligations.

Moreover, based on the provisions of the proposal for Order mentioned above, **it was considered that**, although it is issued under the provisions of the Fiscal Procedure Code, the **publication by the National Agency for Fiscal Administration, on the Internet, of the List of debtors** – natural persons outstanding tax obligations to general consolidated budget and the amount of these obligations (Annex no. 2) **is likely to affect the right to privacy in relation to the necessity to respect the principles of proportionality and non-excessivity of personal data processing**.

In light of the above, the national supervisory Authority has submitted to the National Agency for Fiscal Administration the proposal to amend the provisions of the Fiscal Procedure Code on the publication of lists of debtors natural persons (Article 162 of the Tax Procedure Code), so that data subjects, debtors, are not exposed to public opprobrium and to ensure a real respect for privacy and data protection.

In this regard, it was considered that posting the mentioned list on the website of the National Agency for Fiscal Administration and the disclosure of personal data of debtors to the general public on the Internet, exceed the scope of "collection of taxes", which is achieved by other specific means.

In this context, it was stated that Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC (General Data Protection Regulation), with a direct applicability in all EU Member States, entered into force.

It was highlither that, according to accountability principles provided by Regulation (EU) 2016/679, the data controller is not only responsible for compliance with all principles of data processing ("lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", as well as "integrity and confidentiality"), but it is necessary to be able to demonstrate compliance with those principles.

- **The Ministry of Home Affairs submitted the request of proposals and observations with reference to the proposal for a Law on the use of passenger name record for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, as well as the prevention and removal of threats to national security**

With reference to the proposal of law mentioned above, our institution formulated the following observations and proposals:

The national supervisory Authority reiterated the assessments expressed in previous correspondence on this legislative initiative, namely that implementation of such a system for collecting and processing the passenger data involves a large-scale personal data processing and may represent a new risk to protection of personal data of individuals and thus to respect and guarantee of their fundamental rights, especially the right to privacy.

At the same time, the implementation of such a system involves the collection of a large volume of data, which is why it must be shown clearly that this system is necessary, legitimate and proportionate and that its objective can not be achieved through a system which is less intrusive to privacy.

The legality of this system must be assessed having regard to the principles enshrined in the Charter of Fundamental Rights of the EU, especially in Article 7 on the right to private and family life and Article 8 on the protection of personal data, two different and complementary rights guaranteed by the Charter and in Article 8 of the Convention on Human Rights and Fundamental Freedoms.

In the same time, it was stressed the importance of the 2014 decision of the Court of Justice of the European Union, which invalidated the Data Retention Directive as "the EU legislature exceeded the limits imposed by the principle of proportionality in light of Articles 7,

8 and 52 (1) of the Charter." These issues were also considered by the Romanian Constitutional Court declaring the Law no. 82/2012 to be unconstitutional.

Also, we recalled that the principles of necessity and proportionality of the system can be shown only after assessing the functionality and utility of existing systems scale where a wealth of information is processed.

Therefore, when proposing and designing a new system on a large scale, it must respect the principles of necessity, proportionality, accountability (accountability principle), data protection impact assessment, privacy by design, privacy by default, purpose limitation and rules for data breache notification. These issues are in line with the new Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on the protection data) whose provisions are directly applicable in all Member States of the European Union, starting with the 25th of May 2018.

It was also considered it necessary to analyze the impact on fundamental rights, as well as the data protection safeguards.

In this context, it is recalled that the aspects outlined above have been subject to the address of the Article 29 Working Group (joining all authorities for data protection in the Member States, groupt established by the European Commission) submitted to the LIBE Committee of the European Parliament with reference to EU passenger data system, drawing the attention mainly on the following: demonstrate the necessity for an EU PNR system, respectively to ensure the proportionality of data processing.

On the content of the proposal, our institution issued the following observations:

With reference to the provisions of Directive (EC) 2016/681, it was stressed that the purpose of the law on "prevention and removal of threats to national security" is not within the scope of its regulation.

On the contrary, the above Directive mentions that its scope is quite limited and, in accordance with the proportionality principle, the Directive does not go beyond what is necessary to achieve those objectives.

However, Directive (EU) 2016/681 provides that its application "should ensure full respect for fundamental rights, the right to privacy and the principle of proportionality".

The Directive also provides that Member States are obliged to ensure that an independent national supervisory authority is responsible for advising and monitoring of the processing of PNR data.

Bearing in mind the above-mentioned legal provisions and with reference to the purpose of "prevention and removal of threats to national security" provided by the title of the law and Article 18 letter b), we concluded that national supervisory Authority would have limited powers, by being unable to fulfill its powers in their entirety, by not respecting, in the same time, its independence requirements imposed by the Directive (EU) 2016/681.

According to Article 1 (2) of Directive (EC) 2016/681, "PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2)". In these provisions we cannot found the phrase "removal of threats to national security", they refer exclusively to the processing of PNR data to prevent terrorist activities or serious crimes.

In addition, based on the provisions of the law that established the powers of UNIP, the purpose mentioned aboce contradicts with them, leaving to the interpretation that UNIP fulfills both purposes specified in Article 18 (including the one provided by Law no. 51/1991), although it is organized within the General Inspectorate of the Border Police and acts as data controller of personal data, thus falling under Law no. 677/2001.

In view of the above, it was considered necessary to reassess the extension of the scope of the law to the one established by Directive (EC) 2016/681 and the implementation in accordance with its provisions and with the ones ofLaw. 677/2001, by removing it from the text of the normative act.

At the same time it was shown that it is necessary to eliminate point 1 of Annex to law which establishes the list of offenses relating to "crimes against national security", point which is not found in Annex II of the Directive, appendix referring to the list of serious crimes.

Also, regarding the applicability of the law also to intra-EU, as stipulated in Article 1 (1) a), this is an exceptional measure that can be taken only under the conditions of Article 2 of Directive (EC) 2016/681, and it is likely to affect the principles of proportionality and necessity, mentioned above, by having negative effects on the right of the privacy of EU citizens.

In terms of categories of passenger data, which can be found in Article 14, by taking into account the opinion of Article 29 Working Group (WP 181/2011), we considered the list of items of passenger data to be excessive. Moreover, as stated by the European Commission, PNR data are data unchecked. In other words, they are neither complete nor completely accurate, something that does not comply with one of the principles of protection of personal data, respectively the personal data which are intended to be processed must be accurate and, where necessary, updated.

Moreover, this list is added by default additional information, although not expressly contained in Article 14 (1), they can be derived from certain categories of data such as, for example, in letter j) "travel status ..." or letter s) " all historical changes to the PNR listed in letters a) -r) ". Thus, information on religious beliefs, state of health etc. can be obtained, thus, implicitly, more data than those already established, including sensitive.

Referring to Article 17 of the proposal, this provision should be deleted because the monitoring powers of UNIP contravene Article 15 of the Directive, representing an overlap with the investigatory powers of the national supervisory Authority and, as such, a serious interference in its powers established under the current regulations.

Regarding the competent authorities set out in Article 11 (1), for the clarity of the disposition, it is necessary to specify the exact name in letters a) -d), including by mentioning the public authority where the divisions / departments concerned are organized.

It was also requested to reconsider the establishment of the Romanian Police within the scope of the competent authorities (letter a), based on Article 5 of Law no. 218/2002, republished, which includes also educational institutions for training and continuous training of personnel, as well as other units required to perform specific tasks police, established by law.

The same requests were addressed also on Romanian Border Police (letter b), based on Article 6 of the Emergency Ordinance no. 104/2001, as amended, which makes references to educational units or institutions, training centers, centers, offices and points of contact, as well as other units.

On Article 11 (1) letter i) of the proposal, it was recommended its review and, therefore, the deletion of this authority fromm the scope of the competent ones, given the motivation of the explanatory memorandum to the law referring to the powers of ANAF - General Customs Directorate on the supervision and customs control of goods, issues which do not circumscribe the scope of the Directive (EU) 2016/681.

On Article 42 (3) of the proposal, it was suggested the deletion of "a case of technical failure for a short period" because we consider that it can not be assimilated to force majeure in relation to the obligations of the data controller under Article 20 of Law no. 677/2001, respectively taking the necessary measures including the one referring to the accidental destruction and loss of data.

Regarding the sanctions regime, it was noted that it is contrary to Article 41 which sets out the competences of national supervisory Authority regarding the monitoring of data processing in the PNR system, but also with Article 15 (supervisory Authority) in relation to Articles 4-6 (i.e. Passenger Information Unit - PIU) of Directive (EC) 2016/681 and with Article 35 of Law no. 677/2001. Or, the provisions of Article 42 (1) letters a)-c) relate to data processing operations which air carriers (data controllers) must comply with, aspect which fall within the exclusive competence of the national supervisory Authority.

Consequently, it was shown that Article 42 (5) and (6) are required to be reviewed and modified in accordance with the Directive (EU) 2016/681 and Law no. 677/2001, so that the finding and imposing sanctions rests within the exclusive competence of the national supervisory Authority.

As result, with reference to the legislative proposal, the national supervisory Authority considered that the implementation of such an evidence system may represent a new risk scenario for the protection of personal data of individuals and, therefore, for compliance and guaranteeing their fundamental rights, especially the right to privacy, family and private life regarding the processing of personal data.

Therefore, the national supervisory Authority **did not support the draft law as it was presented.**

- **The Ministry of Communication and Information Society** requested proposals and comments concerning the text of the **draft law for amending the Government Emergency Ordinance no. 111/2011 on electronic communications, as amended and supplemented**

With reference to the proposal of law mentioned above, our institution formulated the following comments and proposals:

According to Law no. 24/2000 on legislative technique for drafting laws, republished, the explanatory memorandum constitutes the instrument of presentation and motivation of the new proposed regulations. In this regard, it was noted that the legislative proposal is not accompanied by the explanatory memorandum.

It was also noted that while the bill aims at the modification of the general normative framework on electronic communications, from the text presented for analysis it results that, in reality, the enactment would complement the legislative framework concerning the processing of personal data and the protection of privacy in the electronic communications framework regulated by Law no. 506/2004.

Thus, it was noted that the proposal is referring to the retention and storage of data by providers of electronic communications services, when using prepaid cards, which amounts to a restriction of the right to privacy, limitation that can exist only in accordance with Article 53 of the Constitution and in accordance with Law no. 677/2001.

Regarding the proposed text, it was noted that it is necessary to determine the exact scope of personal data to be collected by the providers.

On the specifications in paragraph (13), the text submitted does not present clarity and predictability in that it does not regulated in detail the procedure by which the operation of collecting personal data takes place, including in terms of the obligations of confidentiality and security incumbent to data controllers and data processors, bearing in mind the critics from the Decision of the Constitutional Court no. 461/2014, expressed in this regard.

Also, the wording of the text of the second sentence of the paragraph (13), particularly the phrase "these documents" reveal ambiguity and lead to the interpretation that they relate also to copies of identity documents, so it is necessary to reformulate the text.

On paragraph (14) letter a), the term "subscriber" used creates confusion, whereas according to Emergency Government Ordinance no. 111/2011, as it stands, the subscriber is considered to be also the one receiving prepaid services, so it is necessary to specify the category of end user subscribers from who data is not required. In this respect, it is necessary to analyse and clarify the term "end user" from paragraphs (11) and (12).

Also, regarding the exceptions on the collection means provided in paragraph (14), for subscribers whose data is already stored, it must be taken into account also the observance of the principle that data must be accurate and, where necessary, updated, including in terms of

taking measures to ensure that data inaccurate or incomplete, in terms of the purpose for which they are collected and will be further processed, are erased or rectified.

Regarding the "portability" mentioned in letter c) from paragraph 14), it is necessary to analyse and corroborate the data set by this procedure with the ones established by paragraph 12) in order to avoid the non-uniform interpretation and application in practice.

Concerning the reference in paragraph (15), related to the references of the Constitutional Court Decision no. 461/2014, it was considered that its mention is not sufficient to ensure the necessary guarantees that the state must provide to citizens for exercising their fundamental rights, especially the right to privacy.

Compared to the period of 3 years provided in paragraph (16), it was reiterated its observation according to which it covers all the processing operations and all data set by paragraph (12) from point 2 of the project, in disagreement with the principle of strict data storage period necessary to fulfill the purpose, stated in Article 4 (1) letter e) of Law no. 677/2001. In this regard, we noted that the text is ambiguous and leads to the interpretation that service providers can perform any type of data processing operation, even for a period longer than the one provided by Law. 82/2012 (6 months), declared unconstitutional, and there is no consistency and predictability on how the providers will act. In this regard, we noted that the proposal is inconsistent with provisions of Article 5 of Law no. 506/2004, as amended by Law no. 235/2015, considering that this proposal refers also to electronic communications.

It was also stressed that the law proposal does not expressly provide the access conditions to data for the authorities, as well as the purpose of this access, thus infringing the principle of proportionality, bearing in mind those adopted by the Constitutional Court through its Decision no.461/2014, as well as the provisions of Article 53 of the Constitution which stipulate the conditions of restriction of certain rights or freedoms.

As concequence, the national supervisory Authority considered it necessary to submit the explanatory memorandum which fundaments the legislative proposal, taking into account the restriction of a fundamental right, as well as analysing and reformulating the text in order to establish clear and predictable rules for compliance with the requirements of necessity and proportionality set out in the basic Law and the rules of legislative technique.

- **The Ministry of Public Finance** requested proposals and comments concerning the text of the proposal for a **Government Decision for amending and supplementing the Methodological Norms for the application of Government Emergency Ordinance no. 28/1999 on the obligation of economic operators to use electronic tax cash registers, approved by Government Decision no. 479/2003, accompanied by the Explanatory memorandum**

With reference to the documents submitted, the national supervisory Authority formulated the following comments:

It was noted that the Methodological norms approved by Government Decision no. 479/2003 were issued for the application of Government Emergency Ordinance no. 28/1999. This ordinance regulates the obligation to use electronic cash tax registers and to issue receipts or invoices as appropriate to combat tax evasion, with reference to activity of economic operators and not natural persons who act as buyers of certain goods and services and not pursuing an economic activity.

Meanwhile, the aforementioned ordinance establishes the obligation of economic operators to communicate to NAFA fiscal data generated by the concerned trade operation, and not personal data belonging to individuals in their capacity as consumers.

In this context we emphasized that according to the legislative technique norms, normative acts issued in application of laws or ordinances (in this case a government decision) are issued within the limits and according to rules.

Or, under the draft government decision presented for analysis, it is noted the broadening of tax information strictly necessary to the operation, by adding certain categories of new data, having the nature of personal data, which economic operators are required to collect and process without the consent of the individual concerned and to communicate them to NAFA.

In light of the above, we pointed out that, based on Article 26 of the Constitution, which guarantees the right to privacy, the restriction of a fundamental right can be done only under the terms of Article 53, namely only by law and only if necessary, and the measure should be proportional to the situation that caused it.

Moreover, in accordance with the principles derived from the jurisprudence of the Court of Justice of the European Union, a regulation on the protection of personal data, as this is

provided for in Article 8 of the Charter of Fundamental Rights of the European Union, should set clear and precise rules governing the content and application of that measure and to impose a set of minimum requirements, so that people have sufficient guarantees that preserves effectively their personal data against the risk of abuse and against any access and any misuse of such data.

Therefore, the restriction of a fundamental right can be regulated only by law, and only in the above-mentioned constitutional conditions.

Thus, the establishment of a permanent monitoring of an indeterminate number of individuals, by recording a priori of personal data, regardless of the amount paid or product purchased, may be made only by law and only if that measure is proportionate to the situation that caused it and if it requires such invasion of privacy of the data subjects.

It is also necessary to take into account the interests, rights and freedoms of data subjects, aiming to achieve a balance between fundamental rights and economic interests of the state.

Or, based on the text of the Emergency Ordinance no. 28/1999, republished, from its analysis, we noted that there are no provisions concerning the processing of personal data, such as those contained in the draft methodological norms.

With reference to the mass collection of a multitude of personal data from a potential high number of people, we mentioned that, in its jurisprudence, the Court of Justice of the European Union (Joined Cases C-293/12 and C-594/12) in checking the validity of Directive 2006/24/EC ("Data retention Directive") admits that the reasons behind its adoption are legitimate, the purpose being combating crime and public safety, but notes that the EU legislature exceeded the limits imposed by the observance of the principle of proportionality.

The directive cover all persons, means of electronic communication and traffic data without any distinction, limitation or exception to be operated depending on the objective of combating serious crime.

At the same time, the CJEU ruled that the Directive does not provide sufficient guarantees that would ensure an effective protection of data against the risks of abuse and against any unlawful data access and use.

The same aspects were subject to the analysis of the Romanian Constitutional Court, where, by Decision no. 440/2014, ruled that the provisions of Law no. 82/2012 are unconstitutional, stating that the law does not provide the necessary guarantees for the

protection of the right to intimate, family and private life of individuals whose retained data are accessed.

In this context, it was found that the specifications from Section 5, point 4 of the Explanatory memorandum of the proposal are not supported, meaning that legislative amendments would be contrary to the case law of the Court of Justice of the European Union.

Regarding the statements in Section II on the "Description of the situation", they are not able to justify the need to collect all the personal data determined to be additional to the tax ones, strictly necessary for that purpose, namely to combat tax evasion potentially committed by economic operators, and not by individuals who, in addition, do not undertake any economic activity.

On the provisions of Article 4 (3) of Annex 8 (Annex no. 11 to methodological norms) of the decision proposal on "Connecting remote", which were recommended to be analyzed, is was stated, in particular, that personal data such as "g) card number used for payment; h) the payment authorization code; i) all available details about the identity of the cardholder", communicated to the National Agency for Fiscal Administration, simultaneously with the transmission by the institution accepting the payment transaction, involves the processing of personal data.

In the context of the current legal regulations, the communication of personal data, in the manner prescribed, to the National Agency for Fiscal Administration may pose risks to the fundamental rights of individuals, especially since the generic and equivocal phrase on "all details available about the identity of the cardholder" does not respect the principles of forseability and predictability that must comply with a law, namely establishing, in concrete, the categories of personal data and the need for their collection.

Given the social impact of the proposal, as it is mentioned in the Explanatory memorandum, referring to the "increase of public confidence in the fair use of electronic cash tax registers by economic operators and the fair collection by the tax authorities of taxes to the state budget", it was considered, based on Article 4 (3) of Annex 8 (Annex no. 11 to methodological norms) of the decision proposal, that the data processed by the National Agency for Fiscal Administration, as those at issue, appear to be excessive to the purpose mentioned as "the collection of taxes", which is in contravention with the principles of lawfulness, proportionality and necessity under Directive 95/46/EC and Law. 677/2001.

Or, Article 11 (10) of Law no. 207/2015 – Fiscal Procedure Code provides that "processing of personal data by the central and local tax bodies shall respect the provisions of 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 supplemented."

Thus, both retailers and the National Agency for Fiscal Administration, as data controllers of personal data, must process personal data with the observance of the principles set by Law no. 677/2001, whether data is processed with or without the consent of the data subject.

Therefore, personal data intended to be processed must be processed in good faith and in accordance with the existing legislation, to be collected for specified, explicit and legitimate purposes, to be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed, to be accurate and, where necessary, updated, to be stored in a form which permits the identification of data subjects for the duration strictly necessary to achieve the purposes for which they are collected.

The same considerations on the principle of proportionality of the purpose and the non excessive character of data have been made also regarding the collection of personal data set by point 48 of the proposal, on Article 56 (2) letter a) and (4) letter a).

Moreover, it was noted that transmission of data is done electronically and, in this context, we emphasized that, when choosing the means for processing personal data, it must be taken into account that entities holding data and the ones entering in possession of those data are required to maintain the confidentiality of the processed data and to apply appropriate technical and organizational measures to protect personal data.

Taking into consideration the previous observations, the national supervisory Authority considered that the text of the proposal for a Government decision, submitted for analysis, must be within the normative act under which it was issued, namely the Emergency Ordinance no. 28/1999.

Also taking into account that the restriction of a fundamental right is in question, the right to privacy, it must be considered the need to establish clear and predictable rules for compliance with the requirements of necessity and proportionality set out in the basic Law and the rules of legislative technique.

As result, bearing in mind the protection of individuals whose personal data are processed and, thus, their privacy, the national supervisory Authority **does not support the legislative proposal as presented**.

Section 2 Opinions on various aspects of data protection

a) On the publication photos in the online environment

An association requested the point of view of the national supervisory Authority on the legal conditions for processing personal data, respectively photographs and interviews with people considered to be humanitarian cases.

It was stated the following:

The rule established by Law no. 677/2001, as amended, is that the processing of personal data of an individual (including the disclosure) by another natural or legal person, as data controller, is performed only with the expressed and unequivocal consent of the person concerned.

However, exceptionally, personal data may be processed (including disclosed), in many exceptional cases, without the consent of the person concerned. These situations of strict interpretation and application are expressly mentioned in Article 5 (2) of Law no. 677/2001, for data which do not have a special character (such as name, address, e-mail, telephone number, image, voice) and Articles 7, 8, 9 and 10 of the same law, for sensitive data (eg, data concerning racial or ethnic origin, religious beliefs, trade union membership, health data, personal identification number, offenses or misdemeanors).

Regarding the above mentioned legal texts, based on the content of the letter submitted, we stated that the processing of personal data (image and voice) of some individuals considered by the association concerned as humanitarian cases, do not fall in the cases of exception from the consent.

Consequently, in order to achieve the proposed purpose, namely the posting in the online environment of photos and interviews with persons considered as humanitarian cases, the consent of the person whose case is promoted or, in the situation of the minors, of his legal representative, with a prior information of the person whose data will be processed.

In this context, it was stressed out that the information of the data subjects must be carried out according to Article 12 of Law no. 677/2001, amended and completed. At the same time, it has been shown that it is also necessary to comply with the audiovisual regulations (Law no. 504/2002, Decision no. 220/2011) as regards the respect for human dignity and the right to one's image.

At the same time, since from the content of the address transmitted it was revealed that, for the purpose of keeping a record of the association, the latter intends to collect personal data contained in the identity documents belonging to the persons benefiting from humanitarian aid, it was stated that it is necessary to observe the principle of proportionality of the data provided by the provisions of Article 4 (1) letter c) of Law no. 677/2001. Regarding the intention to make copies of the identity cards belonging to the aforementioned persons, for the same purpose, namely keeping of accounting records, it was stated that by Decision no. 132/2011 of the President of the national supervisory Authority regarding the conditions for the processing of personal identification number and other personal data having a general applicability identification function, it is forbidden to carry out and retain copies of the identity card or of the documents containing them, except for the situations stipulated in Article 2 of this decision (express consent of the data subject/express legal provision/opinion of the supervisory authority).

b) On the publication of different laws or decisions which contain personal data by the Offical Journal and by other websites

According to the provisions of Law no. 21/1991 on Romanian citizenship, both the granting of Romanian citizenship (upon request and/or in case of repatriation) and the loss of Romanian citizenship (by withdrawal or approval of renunciation) are made by Government Decisions, which are published in the Official Journal of Romania.

These decisions contain lists of persons for whom the granting or loss of Romanian citizenship has been approved.

Regarding the publication by other websites of the judgments published in the Official Journal which contain personal data, it was stated that these data can only be disclosed if the data subject has expressly and unequivocally gave his/her consent, according to Article 5 (1) of Law no. 677/2001 or under exceptional conditions provided for in paragraph (2) of the same Article.

With reference to the request for verification, correction of the content of the documents published in the Official Journal, it was stated that this responsibility lies with the issuing authority of the normative act sent for publication in the journal.

However, with respect to the content of the letter, it was stated that the person has the right to ask the administrator of that respective website (www.lege5.ro, www.legislatie.just.ro,

www.monitoruloficial.ro), under Article 15 of the Law no. 677/2001 (right to oppose), to delete the data that he considers it belongs. For the exercise of this right, the data subject will submit to the data controller a written, dated and signed request in which he can indicate whether he wishes the information to be communicated to him at a specific address, which may also be by e-mail or through a mail service which ensures that it is handed over only personally. The data controller is obliged to communicate the measures taken as a result of the exercise of this right, within 15 days from the date of receipt of the application, in compliance with the applicant's possible option of sending the response.

In the same letter it was stated that failure to observe the rights provided by Law no. 677/2001 entitles the data subject to submit a complaint to the national supervisory Authority, in compliance with Article 25 (3) of Law no. 677/2001.

c) On the lawfulness of implementing certain applications for monitoring the consumers' behaviour

It was emphasized that the principles regarding the processing of personal data established by Article 4 of the Law no. 677/2001 shall be complied with, irrespective of whether the data processing takes place on the basis of the consent of the data subjects or on the basis of the exceptions to the consent provided by the law.

Accordingly, the data must be strictly necessary for the fullfillment of the purpose (minimum necessary data), aspect which requires a prior analysis by the data controller, by assessing the necessity to collect the data in order to avoid interference in the privacy of the data subject and to find alternative solutions, less intrusive.

Concerning the consent, the exercise of the data subject's autonomy of will means that, at any time, he/she may withdraw his/her consent for the processing of all or some of his/her personal data, with no negative consequences for him/her, with reference to the marketing activity.

To the extent that the data controller invokes the legitimate interest, it is necessary, on one hand, to substantiate its argument in order to motivate and prove the prevalence of this interest over the rights and freedoms of the data subject and, on the other hand, to inform the data subject about the processing of his/her data.

The information the data subjects must be done regardless of the legitimacy of the data processing, according to Article 12 of the Law no. 677/2001, amended and completed. Within

this information, individuals should be made aware of all the conditions of data processing, including the rights to oppose, access and intervention, and the conditions for their exercise, in order to consent to a certain well-informed processing.

According to the provisions of Article 15 of the Law no. 677/2001, as amended and supplemented, the right to oppose is the right of the data subject to oppose at any time to the processing of his/her data for justified and legitimate reasons, except where there are contrary legal provisions. In the case of justified opposition, the processing may no longer cover the data concerned.

According to the same legal provisions from above, the data subject has the right to oppose at any time, free of charge and without any justification, for his/her data to be processed for direct marketing on behalf of the data controller or a third party, or to be disclosed to third parties for such a purpose.

The guarantee of this right is the expression of the prevalence of the right to oppose over the economic interests of the data controller, especially when using new technologies for its activity, as is the case here.

It was also stated that, according to Article 53 of the Constitution, the exercise of certain rights or freedoms may be restricted only by law. The right to privacy is one of the rights that fall within the category of fundamental rights of the individual, guaranteed and protected by the fundamental Law.

Thus, as regards the restriction of certain rights, Article 16 of the Law no. 677/2001 lays down the conditions under which this may take place, the exceptions being applicable only to the field of criminal law and only for a limited period of time after which the data controllers will take the necessary measures to ensure the respect for the rights of the data subjects and will notify the national supervisory Authority of these situations.

The collection of data of individuals through specialized software is an interference with the fundamental right of their privacy which can lead to serious harm to the right of privacy and may represent major risks for the protection of their personal data, as the data subjects may include also people with disabilities and minors.

It has also been stressed that, prior to the creation and implementation of such a data collection and processing system, it is necessary to ensure an adequate level of data protection (compliance with the principle of privacy by design), all the more it is specified the fact that "those applications work with data from pre or simultaneous video recordings".

In conclusion, as regards the situations presented, since the data controller preestablish the purposes and means of data processing, which is binding, without consulting the data subject, he can no longer rely on the legitimate condition for obtaining the consent of the data subject.

Also, as regards the condition of the legitimate interest, processing can not be based on this exception unless all the above conditions are met, in particular ensuring that the rights of the data subjects are respected (primarily the right to information), as well as the other guarantees regarding the fair and lawful data processing.

As regards the provisions of Article 5 (2) letter b) of Law no. 677/2001, it was stated that they are not applicable to the purposes of advertising, marketing and publicity.

Furthermore, it has been pointed out that the technical supervision by an audio/video surveillance cameras, without the data subject knowing this fact, can only take place under the Code of Criminal Procedure, only under certain conditions expressly laid down by that code. In the same sense it is stipulated by the provisions of Article 5 (2) and (3) of Decision no. 52/2012, according to which the surveillance cameras are placed in visible places, and the use of hidden surveillance means is forbidden, except for the cases provided by law.

Therefore, such types of specialized software, as those presented in the letter, cannot be implemented by data controllers in the field of advertising, marketing and publicity, except for the situations which are in compliance with all national and European legal provisions on personal data protection.

Regarding the relevant European regulations, it was clarified that the proposal for a Data Protection Regulation stipulates that any data subject should have the right to know and to communicate to him/her, in particular, the purposes for which the data are processed, if possible for what period, the identity of the data recipients, which is the logic of automatic data processing and which could be, at least if it is based on profiling, the consequences of such processing.

d) On the disclosure of debtors natural persons data

As regards the disclosure by the tax authorities of the data of the debtors natural persons, it has been pointed out that the said processing operations can only be carried out based on the consent of the data subject or only under the legal conditions of exception from consent, of strict interpretation and application, in compliance with the principle of proportionality of purpose, enshrined in Article 4 (1) letter b) of Law no. 677/2001.

By the judgement of Case Smaranda Bara and others (C-201/14), the Court of Justice of the European Union held that Articles 10, 11 and 13 of Directive 95/46/EC must be interpreted as precluding national measures allowing a public administration authority of a Member State to transmit personal data to another public administration authority that will further process such data without the data subjects having been informed of such transmission or processing.

Therefore, the requirement for a fair processing of personal data provided in Article 12 of Law no. 677/2001, which implements Article (6) of Directive 95/46/EC requires an authority of the public administration to inform the data subjects about the transmission of these data to another public administration authority for a further processing by the latter as recipient of those data.

With regarding this aspect, the national supervisory Authority emphasized that the right guaranteed by Article 12 of the Law no. 677/2001 must be respected by all personal data controllers, irrespective of the legitimacy of the data processing, namely consent or exceptions, according to the provisions of Article 5 of the Law no. 677/2001.

The national supervisory Authority drew attention to the need to respect the right to information of the data subject, both in terms of the information which must be made available to the data subject and the subsequent exercise of the other rights by the data subject, such as the right of access to data, right of intervention upon data, right to oppose, in order to enable the individual to use the legal means accordingly.

It was pointed out that Law no. 677/2001 lays down certain obligations for personal data controllers, including the processing of legitimate processing (Article 5), the information of the data subjects (Article 12) and respect for the rights of individuals those data they process (Articles 13-18), as well as the obligation to ensure the confidentiality and security of data processing (Articles 19 and 20).

It was emphasized that all of the above were not taken into account when issuing Order no. 558/2016 regarding the Procedure for publishing the lists of debtors who register outstanding tax obligations, as well as the amount of these obligations, bearing in mind that Article 11 (10) of Law no. 207/2015 - The Fiscal Procedure Code provides that: "The processing of personal data by the central and local tax bodies is carried out in compliance with the provisions of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as amended and supplemented."

It was stated that the national supervisory Authority was not consulted, according to the provisions of Article 21 (3) letter h) of Law no. 677/2001, in connection with the proposal for Order no. 558/2016 on the Procedure for publishing the lists of debtors who have outstanding tax obligations, as well as the amount of these obligations.

Regarding the content of this Order, it was highlithed that it does not contain provisions regarding the observance by NAFA of the obligations stipulated in Article 12 of the Law no. 677/2001, of the rights of the data subject or of the security measures of the processing.

It was considered that, with reference to Article 162 of the Fiscal Procedure Code, in application of the principle of proportionality and minimization of data, provided by Article 4 of Law no. 677/2001, the publication of the person's tax domicile is excessive.

e) On the legal conditions concerning the biometric applications

The rule established by Law no. 677/2001, as amended and supplemented, is that the processing of personal data of a natural person by another natural or legal person, in its capacity as a data controller, is carried out only with the expressed and unequivocal consent of the person concerned.

The same law also expressly establishes certain exceptions from the obligation to obtain the consent in the case of processing of personal data. Among these exceptions, covered by Article 5 (2) of Law no. 677/2001, amended and supplemented, it is included the one in which the processing is necessary for the fulfillment of a legal obligation of the data controller or for the accomplishment of a legitimate interest of the data controller or of the third party to whom the data are disclosed, provided this interest does not prejudice the interest or fundamental rights and freedoms of the data subject.

The principles on the processing of personal data set out in Article 4 of the Law no. 677/2001 shall be complied with, irrespective of whether the data processing takes place on the basis of the consent of the data subjects or on the basis of the exceptions to the consent provided by the law.

It has therefore been made clear that biometrics may be processed under the above legal provisions but only if this measure is proportionate to the risks faced by the data controller and determines the taking of such intrusive measures in the privacy of individuals concerned. At the same time, their interests, rights and freedoms must also be taken into account.

Depending on the specific nature of the processing, it is necessary to identify an alternative way of accomplishing the proposed purpose by identifying other data whose processing does not pose a risk to the private life of the individual.

Insofar as the implementation of such a system affects the rights of the data subjects as employees, in addition to the provisions of Law no. 677/2001, as amended and supplemented, the provisions of the Labor Code or other regulations referring to their status must be observed. In this respect, prior to the implementation of the system, a thorough justification is required for taking this measure at the same time as consultation with the trade union or employees' representatives.

In this context, it has been stated that in several situations where employers have implemented, for example, a system for establishing the working hours based on biometric data (fingerprints) of employees, without a strong justification for the need to take this measure, they have been sanctioned by the national supervisory Authority, and the courts have maintained the measures taken by our institution.

f) On the creation and publication of the evidence of certain employees

A natural person has requested the point of view on the creation, as well as posting on the Internet, of a database of problem-employees, employees who have created certain problems at work, including name, surname, age, photograph, home city, occupied position, facts and any other information considered useful.

According to the provisions of Article 5 (1) of the Law no. 677/2001, as amended and supplemented, the basic principle governing the processing of personal data (including data collection and disclosure to third parties) is the expressed and unambiguous consent of the data subject.

Exceptionally, however, personal data may be processed by a data controller, without the consent of the data subject, in a number of exceptional situations, of strict interpretation and application, covered by Article 5 (2) of Law no. 677/2001.

Therefore, the personal data referred to in the content of the letter transmitted (name, surname, age, image, home city, function, occupation - of employees/former employees of entities) can not be disclosed by employers/former employers (who have the capacity of data controllers, as defined by Law 677/2001), except for the case where there is the consent of the

data subject or, exceptionally, only in the legal conditions of exception from consent, of strict interpretation and application, in compliance with the principle of proportionality of purpose.

In addition, it has been pointed out that Article 10 of Law no. 677/2001 legitimizes the processing of data relating to criminal offences or contraventions or to administrative or contravention sanctions imposed on the data subject only by or under the control of public authorities within the limits of the powers conferred by law and under the conditions laid down by the special laws governing such domains.

In light of the above, taking also in cosideration:

- Recital (53) Directive 95/46/CE according to which certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose, such as that of excluding individuals from a right, benefit or a contract;
- the harmonised opinion of the supervisory authorities from the Member States expressed in the Working Document on blacklists no. 65 of 3rd of October 2002, adopted by Article 29 Working Group of the European Commission, according to which the lists containing data of employees or job candidates on their reprovable professional behaviour may have a high impact on the interests of the data subjects that on these "blacklists", which is why they need a special protection;
- the provisions of Article 8 of the Convention for the protection of human rights and fundamental liberties which proclaims the respect for the private and family life of any person and those of Article 26 of the Constitution guaranteeing the respect for the fundamental right to intimate, family and private life, as also confirmed in the Charter of Fundamental Rights of the European Union;
- the necessity of ensuring an efficient protection of the right to privacy of employees and the observance fo the principle of proportionality of the processing;

it was emphasized that the processinf personal data for the mentioned purpose, namely for the creation of a "blacklist" cu "problem-employees", is an excessive processing in connection with the purpose pursued and the provisions of Article 4 of Law no. 677/2001.

g) On the processing of data by video surveillance systems

An entity of professional notary requested the approval of the national supervisory Authority for the processing of personal data of employees by means of video surveillance, pursuant to Article 8 (3) of the Decision no. 52/2012.

The national supervisory Authority, in the context of the claims of the company and the need to ensure an effective protection of employees' right to privacy, in relation to the determined, explicit and legitimate nature of the purpose and proportionality of the processing, with reference to the request for an opinion under Article 8 (3) of the Decision no. 52/2012, it considered that the supporting evidence submitted did not justify the approval.

Thus, it was appreciated that there are no arguments for the processing of personal data (images) of employees in the offices of the entity of professional notary, by using a video surveillance system, in relation to the activity performed and the legal obligations of this company.

It has been stated that, following the content of letter submitted, the request for the installation of the video recording equipment is justified in order to prevent possible theft offenses which has been recorded both at that office as well as at the premises of other notarial offices.

Therefore, as regards the need to ensure an effective protection of the right to privacy of employees and the determined, explicit and legitimate nature of the purpose and proportionality of the processing of their personal data, it was considered that the elements presented in the submitted letter did not meet the conditions stipulated by Article 8 of the Decision no. 52/2012.

- **Opinions on cases from the Court of Justice of European Union**

In 2016, the national supervisory Authority submitted its opinions to the Ministry of Foreign Affairs in several cases pending before the Court of Justice of the European Union concerning the interpretation of certain articles of Directive 95/46/EC, as follows:

- **Case C-13/16** on the interpretation of Article 7 letter f) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- Case C-73/16 on the interpretation of Article 7, 8 and 47 of the Charter of fundamental rights of EU, as well as of Article 1 (1), Article 7 letter e), Article 13 (1) letters e) and f) and Article 17 (1) of Directive 95/46/EC;

- Case C-434/16 on the interpretation of Decision of the Court of Justice in Digital Rights Ireland and Seitlinger, in the connected cases C-293/12 and C-594/12 (including especially points 60-62).

Section 3 The representation activity before courts of law

In view of finalizing certain court actions favourable to our institution, as a result of their promotion by some data controllers sanctioned by the national supervisory Authority during 2016, we present below some relevant cases:

- **Decision pronounced in a dispute over the transmission of debtors data by a non-banking financial institution**

The national supervisory Authority has been notified by a natural person that, following the conclusion of a credit card contract, negative data about him/her were reported to SC Biroul de Credit SA by the non-banking financial institution, although he/she has not been notified 15 days prior ot the transmission of his/her data to SC Biroul de Credit SA. The person mentioned that he/she addressed this institution through several petitions by e-mail requesting the deletion of his/her data from SC Biroul de Credit SA, but is unsatisfied with the answers he/she received.

Our institution started an investigation at that entity in order to verify compliance with the provisions of Law no. 677/2001, including the ones notified.

The national supervisory Authority issued a report on the findings/sanction that the data controller committed the contraventional act of unlawful processing of personal data provided by Article 32 of the Law no. 677/2001, infringing Article 8 (2) of ANSPDCP Decision no. 105/2007, as well as Article 12 of the Law no. 677/2001. Thus, the non-banking financial institution reported negative data to SC Biroul de Credit SA for two years, without submitting evidence of prior notification to the data subject, 15 days prior to the transmission of his/her data, in none of the ways provided by Article 8 (2) of ANSPDCP Decision no. 105/2007.

The report of the findings/sanction was challenged in court by the sanctioned data controller, requesting the annulment of the report and ordering our institution to pay the costs.

The court dismissed the data controller's complaint, arguing that "the investigating officer made a fair individualization of the sanction of the offense by applying the sanction of the warning."

The non-banking financial institution filed an appeal against the decision of the court of first instance which was rejected by the higher court, the solution remaining final in favour of the national supervisory Authority.

The irrevocable decision of the court confirmed the approach of the national supervisory Authority to respect the legitimacy of the processing of personal data.

- **Decision pronounced in a dispute over the unlawfull processing of personal data by a hotel unit**

The national supervisory Authority carried out an investigation to a data controller from the hotel sector with the purpose of verifying the compliance with the provisions of Law no. 677/2001 and of Law no. 506/2004. Following the investigation, it was found that the data controller processes data for the purpose of providing hotel and tourism services, as well as for advertising, marketing and publicity purposes.

The national supervisory Authority has issued a report of a findings/sanction ascetaining that the data controller has committed the following offenses:

- failure to notify and malevolent notification, contravention provided by Article 31 of Law no. 677/2001, under the form of failure to notify under the conditions of Article 22 of Law no. 677/2001, because it did not notify the processing of personal data for hotel and tourism services, for advertising, marketing and publicity, as well as for video surveillance, although it had this obligation before the commencement of processing;
- illegal processing of personal data, contravention provided by Article 32 of Law no. 677/2001, by infringing the provisions of Article 12 of Law no. 677/2001, modified and supplemented, and of Article 5 (1) of Law no. 677/2001, modified and supplemented, because the data controller, at the time of writing the report, could not provide any evidence of informing the data subjects according to Article 12 of the Law no. 677/2001, for the processing of personal data which it carries out for the purpose of hotel and tourism services and for the purpose of advertising, marketing and advertising;
- failure to fulfill the obligations regarding the confidentiality and enforcement of security measures, contravention provided by Article 33 of Law no. 677/2001, modified and supplemented, by failing to fulfil the obligations on the implementation of confidentiality and security measures for the processing provided by Article 20 of Law no. 677/2001,

modified and supplemented, because the data controller did not establish and implement a policy/procedure on the minimum security measures for the processing of personal data it carries out, and the employees with tasks related to the processing of personal data were not trained on the provisions of Law no. 677/2001 and the risks involved in the processing of personal data;

- non-compliance with the conditions provided by Article 4 (5) of Law no. 506/2004, modified and supplemented, as the data controller, on its own website, for the information stored and accessed at the level of the terminal device of the user, has not cumulatively fulfilled the conditions provided by Article 4 (5) letters a) and b) of Law no. 506/2004, modified and supplemented, respectively obtaining the user's consent for the existing cookies on the website and providing, prior to expressing the consent, the information about the general purpose of processing the stored information, the lifetime, the information stored and accessed, as well as allowing third parties to store and/or access the information stored in the user's terminal equipment, contravention provided by Article 13 (1) letter i) of Law no. 506/2004, amended and completed.

For the deeds presented in the report of the findings/sanction the data controller was sanctioned with 3 contravention fines and a warning.

The report of the findings/sanction was challenged before the court by the data controller in terms of the contraventions withheld for the data controller.

The complaint of the data controller was dismissed by a final court order.

Thus, the court of appeal held that "The acts committed are aggravated as it is a cumulation of deviations, and the legislator did not intend to cause damage, but to sanction a possible social danger (...)".

The final decision of the court of appeal confirms the fair interpretation given to the provisions of Law no. 677/2001 and Law no. 506/2004 by the representatives of the national supervisory Authority and, consequently, the fair individualization of the sanctions withheld for the above mentioned data controller.

- **Decision pronounced in a dispute over the processing of biometric data by a public institution**

The national supervisory Authority conducted an ex officio investigation to a data controller from the public sector regarding a press statement, stating that the working hours of hundreds of officials within the controlled data controller were established based on fingerprint.

As a result of the control carried out, the national supervisory Authority found that access of part of the data controller's employees to the institution was based on the personal digital fingerprint.

Prior to the procurement and implementation of the electronic system for establishing the working hours, the data controller used access cards for employees in order to access the institution.

For the implementation of the electronic system for establishing the working hours, the data controller collected the biometric data (fingerprints) of the employees. Thus, through the electronic system for establishing the working hours, the hours of starting and ending of the daily activity, as well as entries/exits from the institution were recorded.

When the investigation was carried out, about 500 people were employed within the investigated data controller, but only half of them used the access card.

Also, at the time of the inspection, it was ascertain that 755 people were recorded in the system, of which only 500 were employed and the others were retired and/or terminated their work relationship with the data controller. However, the system retained the data of the persons (i.e. the single number assigned when hi/she was an employee of the data controller, the surname, the name, the date and time of the entry, the date and time of exit and the personal identification number), although they no longer had employment relationship with that employer.

The investigating data controller did not submit any document approving the electronic system for establishing the working hours nor an assessment of the the necessity for the implementation of this system.

When the control was carried out, there was no evidence of prior notification of the employees on the electronic system for establishing the working hours, there was no evidence of employees' consent to the implementation of this system, no data storage period established, no sufficient confidentiality and security measures were adopted for the processed data (biometric data), so that the data controller violated the provisions of Law no. 677/2001.

The acts committed by the data controller have been sanctioned by a fine and the report of findings/ sanctioning contravention has been challenged in court.

The court, by analyzing the evidence in question, found that the report of the national supervisory Authority was legally drawn up, so that the applied sanctions were maintained.

The judgment remained final, thus dismissing the appeal of the data controller.

- **Decision pronounced in a dispute over the video surveillance by a public institution of the employees in offices**

The national supervisory Authority was notified by a natural person on the fact that a public institution, as employer, processed his/her personal data, images, through video surveillance system, installed including in the working places (offices), without complying with the legal provisions.

An investigation was started at the respective institution in order to verify the compliance with the provisions of Law no. 677/2001, including the above mentioned aspects.

The national supervisory Authority has issued a report of a findings/sanction ascetaining that the data controller has committed the following offenses:

- failure to notify and malevolent notification, provided by Article 31 of Law no. 677/2001, under the form of failure to notify under the conditions of Article 22 of this law;
- illegal processing of personal data, provided by Article 32 of Law no. 677/2001, because the data controller did not inform the data subjects whose images are processed through the installed video surveillance system, according to the provisions of Article 11 of Decision no. 52/2012;
- illegal processing of personal data, provided by Article 32 of Law no. 677/2001, because the data controller processed in an excessive way the personal data, namely the image of its employees, through the video surveillance cameras installed in 9 offices and an auditorium room, infringing Article 4 (1) letters a) and c) of Law no. 677/2001, with reference to Article 8 of Decision no. 52/2012.

The report of the findings/sanction was challenged before the court by the sanctioned public institution, demanding the annullment of the report.

The court dismissed the complaint, noting that, on one hand, on the date of the inspection, the controller had not made the prior notification, according to Article 22 of the Law no. 677/2001 and, on the other hand, the monitoring of persons, premises and property carried out within the data controller, even if it was carried out only for the purpose of ensuring the

protection of the objective, goods and persons and the prevention of acts like the evasion of certain goods, does not remove the obligation of notification referred to in Article 22 of the Law no. 677/2001, since this surveillance poses risks to the fundamental rights and freedoms of employees, especially the right to privacy.

With regard to the second offense, the court found that it existed and was duly taken into account by the investigating officer, in the circumstances in which the applicant made the decision to establish the surveillance cameras without first consulting the central authority in domain and without consulting directly and explicitly the employees, which leads to the conclusion that it has acted outside the national and international law.

It was noted that the applicant's allegations that employees were aware of the existence of surveillance cameras because they were informed, under signature, of their decision to install the surveillance system are not equivalent to direct information of the employees about the processing of their data. The court held that the information had to be made in a complete and clear manner.

As regards the third offense, the court found that it was legally and thoroughly withheld from the applicant once the employees are permanently monitored and supervised with surveillance cameras installed in the offices and in the audience room, thus experiencing in-work pressure and a discomfort.

The court of first instance took the view that the measure taken by the applicant to install these surveillance cameras was disproportionate to the stated purpose of ensuring the protection of the objective, the goods and persons and the prevention of acts of misappropriation in respect of fundamental rights of its employees.

The applicant filed an appeal against the decision of the court of first instance, which was rejected by the High Court, the final decision being in favour of the national supervisory Authority.

Section 4 Public information

During 2016, the national supervisory Authority continued the activities and modalities of communication aimed at informing the general public about the specific rules for the processing of personal data.

Thus, the European Data Protection Day was organized, as every year, a prestigious event that was honoured by the presence of leading representatives of central public authorities, civil society and the private environment.

An important role in the popularization of the field of data protection was also played by the broadcasting of a personal information clip on the public television post.

Throughout the year, our institution has actively participated in the most important data protection events organized by various public institutions or private entities. At these meetings, the representatives of the national supervisory Authority have clarified certain aspects on the conditions of use of the data, the respect of the rights of data subjects and the confidentiality of personal data processing.

Among the significant events in which our institution was involved, we emphasize:

- ✓ **European Data Protection Day**

On 28th of January 2016, we celebrated the 35th anniversary of signing, in Strasbourg in 1981, the Convention 108 on the protection of individuals with regard to automatic processing of personal data, the first legal instrument adopted in the field of data protection.

To increase the awareness of individuals throughout Europe on the importance of protecting personal data and specific rights, the national independent data protection authorities in the European states are organizing specific events.

For the celebration of the European Data Protection Day, the national supervisory Authority organized a symposium at the Palace of Parliament, which enjoyed the prestigious participation of senior officials and representatives of the judiciary, academia and non-governmental organizations.

On this occasion, our institution presented the new data processing notification regime, established by the Decision no. 200/2015 of the national supervisory Authority.

- ➢ **Data Protection Conference – solutions and responsibilities**

On the 23rd of June 2016, the Conference Data protection – solutions and responsibilities took place at the Chamber of Commerce and Industry of Romania where the Minister for the Communications and Information Society gave a short presentation in the opening of the event.

With the occasion of this event, where several guests from the private and public sector participated, the implications of the new General Regulation on Data Protection adopted by the

European Parliament and Council were analyzed and the representatives of the supervisory authority presented the novelties brought by the new European regulation with a direct application.

As it was organized in an interactive manner, this event highlighted the real interest of legal persons for the compliance with the requirements of the new Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, applicable starting with the 25th of May 2018.

- **Reunion in the medical and pharmaceutical sector**

On the 28th of November 2016, a reunion of the companies interested in the processing of personal data in the medical and pharmaceutical sector took place.

During this event, the representative of the national supervisory Authority presented the main rules applicable in the medical sector, as well as the novelties brought by Regulation (UE) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, applicable starting with the 25th of May 2018.

At this reunion, the representative of the Pharmacists College in Romania underlined the particularities and the importance of using personal data in the pharmaceutical sector, as well as the current practical difficulties.

In the same time, the representative of private sector highlighted the internal measures necessary for each data controller in order to evaluate the risks and to ensure the confidentiality of the data kept, including the measures to be taken for the applicability of the new European legal framework.

- **Round table in direct marketing sector**

The representatives of the national supervisory Authority attended the round table organised by the Romanian Association for Direct Marketing (ARMAD) on the 14th of April 2016.

Within this event, the issue of personal data processing in the field of direct marketing was addressed, including the implications of the adoption of the General Data Protection Regulation, as well as the security of personal data processing, in the context of the current technological evolution, with reference to the wide internet for commercial communications.

Beyond these events, the website of the national supervisory Authority continued to be an effective and useful mean of informing data controllers and the general public about developments in the field and the work of our institution.

In order to popularize the activity of the institution and the specific regulations in the field, press releases were published, presenting significant aspects of the control activity or other events involving the National Supervisory Authority. Also, information was provided by telephone and audience at the premises of the national supervisory Authority, the citizens and data controllers were informed in a quick and efficient manner, namely they have been provided in a direct way with useful information on the rights of data subjects and obligations specific to data controller, clarifications regarding the conditions of data processing and their disclosure to third parties.

The press articles published and the news broadcasts on the main TV posts have reflected the interest shown by the media in the field of personal data protection.

CHAPTER IV

THE CONTROL AND SOLVING COMPLAINTS AND NOTICES ACTIVITY

Section 1 Overview

An important component of the activity of the national supervisory Authority is the monitoring and control of the lawfulness of personal data processing through investigations conducted either ex officio or in order to solve complaints and notices received.

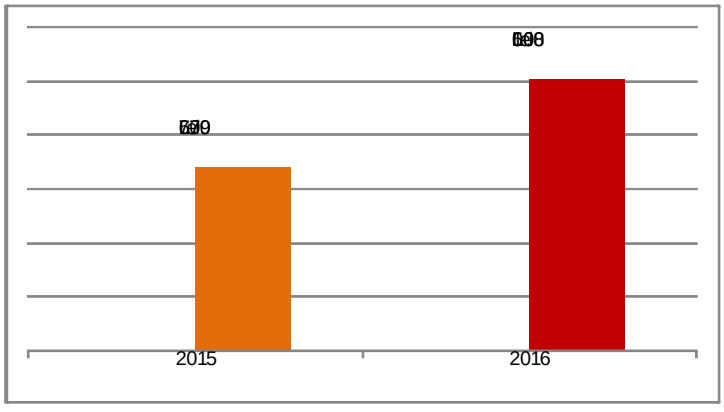
In 2016, the ex-officio investigations were focused primarily on compliance with legal provisions applicable to the processing of personal data within the systems of evidence such as credit bureaux, biometric data processing and data processing by public authorities.

Concerning the handling of complaints and notices, in the context of a considerable increase in their number (**2014 complaints and 188 notices**), in 2016 the notices were referring mainly to violations of financial and banking legislation, within the systems using means of video surveillance or in the electronic communications sector.

The total number of investigations carried out by the national supervisory Authority in 2016 is **632**, with an increase of 57% over the previous year.

Following the investigations carried out, contravention sanctions were applied consisting of **193 fines and 357 warnings**.

The total amount of the fines applied in 2016 was **1,008,500 lei**, with an increase of 48% over the previous year. (figure 1)



Section 2 Ex-officio investigations

In 2016, the national supervisory Authority undertook **140 ex-officio control actions**, both in the public sector and in the private sector. Thus, **62 warnings and 72 fines** were applied in a total amount of **648,500 lei**.

I. Compliance with the provisions of Law no. 677/2001 and Law no. 506/2004 regarding the processing of personal data within evidence systems such as credit bureau (Banking/Non-banking financial institutions)

The large number of complaints and notices received in 2015 by the national supervisory Authority on personal data processing within evidence systems such as credit bureau led to the ex-officio investigations to the banking and non-banking financial institutions participating in the evidence system of the credit bureau. A number of **24 entities** that processed personal data in evidence systems such as credit bureaux were subject to control, and the total amount of sanctions applied was of **382,000 lei**.

The controls carried out were aimed at verifying the compliance with the provisions of Law no. 677/2001 and Decision no. 105/2007 regarding the processing of personal data performed in an evidence system of credit bureau type systems, especially regarding the respect of the rights of the data subjects.

During the inspections carried out, our institution requested information regarding the clients' credit reports which were reported to the credit bureau with outstanding debits, the notifications (information) sent to the clients that are to be reported, according to the Decision no. 105/2007, as well as the proof of the transmission of these notifications.

As a result of the investigations carried out, it was found that most of the banking/non-banking financial institutions subject to control reported to the credit bureau without complying with the legal provisions, thus 23 out of the 24 controlled entities were sanctioned.

The main deficiencies found in the activity of processing personal data carried out by the banking/non-banking financial institutions in the evidence system of credit bureau type systems were the following:

- the transmission of negative data by infringing the provisions of Article 5 (1) of Decision no. 105/2007, which provides that negative data are to be transmitted to credit bureau type filling systems 30 days after the debt enters into force;

- the transmission of negative data by infringing the provisions of Article 8 (2) of Decision no. 105/2007, which provides that negative data are to be transmitted to the credit bureau type filling systems, only after a notice has been sent in advance by the participants to the data subject at least 15 days before the day of the transmission;
- the notifications (information) transmitted to clients on the fact that they are to be reported with outstanding debts do not comply with the provisions of Article 9 (1) of Decision no. 105/2007.

With reference to the aspects ascertained after the inspections carried out, the following were recommended to the banking and non-banking financial institutions:

- to adopt the necessary measures in order to comply with all the provisions of Decision no. 105/2007 regarding the processing of personal data performed in an evidence system of credit bureau type systems;
- to take the measures necessary to delete the information transmitted as negative data to the credit bureau withour the prior information according to Article 8 (2) of Decision no. 105/2007.

II. Verifying the compliance with legal provisions within the processing of personal data such as biometric data

The national supervisory Authority carried out investigations of several entities which processed or intended to process biometric data. Investigations were made ex-officio, both as thematic investigations, as well as a result of the notification of the other departments within the national supervisory Authority.

Biometric data are part of the category of personal data relating to the physiological or behavioral characteristics of a natural person, enabling it to be uniquely identified.

Identifying a person using a biometric system is, usually, the process of comparing a person's biometric data (collected at the time of identification) with a series of biometric models stored in a database, as per Opinion 3/2012 on developments in biometric technologies issued by Article 29 Working Party.

Under the same legislation, within the processing of personal data, the data must be adequate, pertinent and not excessive in relation to the purpose for which they are collected and further processed.

Biometrics-based information technology is mainly used for the secure access to the premises by unlocking doors or turnstiles, authenticating access to logical resources in an information system, unlocking devices (tokens, cards, laptops etc.). Authentication and identification mechanisms involve performing operations such as recording and storing template data, comparing the read results when accessing, registering additional information (e.g., surname, first name or person identifier, eventually the date and time of access). Within these information systems, operations on biometric data must be very secure.

Biometric technologies involve capturing the biometric data of a person, transforming them into a biometric pattern (template/pattern), storing it in a database, and then verifying the identity of that person by comparing biometric patterns (a comparison process of a series of data with multiple data series) with the corresponding physiological/ behavioral characteristic of the individual. When using these technologies, storing and comparing biometric data must be very secure.

Given the widespread use of new technologies in contemporary society, there is a need to analyse their impact on respect for the right to privacy and the principles of personal data processing. This raises the question of the invasive and inappropriate nature of these technologies in relation to certain purposes or activities for which they would be used. Another aspect to be analysed is the security risk of databases containing biometric data.

Regarding the controlled entities, we specify that the majority of them have implemented or intended to implement biometric authentication systems, in particular for establishing the working hours and/or physical access within the entity, based in particular on fingerprints or facial recognition.

The national supervisory Authority has considered that the processing of biometric data is excessive in relation to those purposes, by imposing both fines and recommendations on the identification of less intrusive measures in the privacy of the data subjects. At the same time, the national supervisory Authority has issued decisions on the cessation of biometric data processing and the deletion of biometric data already collected.

There has also been a case in which a biometric system was intended to achieve the facial recognition of individuals, information which should subsequently have been used to prohibit the access of those persons within the entity.

As a result of the investigation carried out, in this case, the national supervisory Authority considered this processing to be excessive and refused the

registration of the notification submitted by the data controller in the Register of evidence of personal data processing of the personal data processing.

"In this context, we stress that the courts have consistently confirmed the approach of the national supervisory Authority namely that the processing of personal data (fingerprints) of employees can be perfomed only on the basis of a thorough analysis of the necessity and proportionality of such measures, and the employer must identify alternative solutions that have a lower impact on employees' privacy.

In relation to this specific issue, the jurisprudence of the European Court of Human Rights referring to article 8 of the Convention on the protection of human rights and fundamental liberties (the right to the protection of private and family life), the European court has stated that the protection granted by this article would be diminished in an inacceptable way if the use of modern scientific techniques is allowed at any cost and without a just balance between the benefits of an extensive use of such techniques and the important interests referring to the private life (Case S. and M. Marper vs. the UK)." – ANSPDCP press release, 08.12.2015.

III. Personal data processing in the public sector – local public authorities (county councils and municipalities)

In 2016, a total of 33 control actions were carried out and 15 warnings and 13 fines were applied. The total amount of the fines applied within the ex-officio investigations of this theme was of 29,500 lei.

The investigations carried out had as objective the verification of compliance with the provisions of Law no. 677/2001, as well as with the provisions of the Law no. 506/2004.

The objectives were:

- the fulfillment of the notification obligation for the processing through video surveillance;
- the means for processing personal data by the county public authorities, under Law no. 677/2001;
- ensuring the rights of the data subjects;
- the fulfilment of the obligation of ensuring the confidentiality and security of processing.

From the investigations carried out, it was found that the administrative-territorial units represented by the mayor or the president of the county council are exempt from the submission of the personal data processing notification forms, according to the ANSPDCP President's Decision no. 200/2015 on the determination of cases of processing of personal data for which no notification is required, as well as for the amendment and repeal of certain decisions. According to Article 3 (3) of the above Decision, the data controllers are required to ensure the rights of data subjects, as well as the confidentiality and security of data.

The investigations revealed that **the administrative-territorial units represented by the mayor** process personal data for the fulfillment of the legal obligations: human resources, hadling petitions and granting of audiences, taxes and duties, finding and sanctioning the contraventions, debt collection/recovery, urbanism and land planning, permit issuance, cadastre and real estate publicity, evidence of persons, monitoring/security of persons, premises and/or public/private goods etc.

It also emerged that **the administrative-territorial units represented by the president of the county council** process personal data for the fulfillment of the legal obligations: human resources, hadling petitions and granting of audiences, issuance of urbanism certificates etc. The data controllers declared that no requests for exercising the rights of the data subjects under Law no. 677/2001, amended and completed, were submitted.

Following the inspections, the following deficiencies were found:

- non-compliance with the obligation concerning the information of data subjects according to Article 12 of Law no. 677/2001,
- non-fulfillment of the obligation concerning the confidentiality and the implementation of security measures,
- failure to notify the purpose of "monitoring/security of persons, premises and/or public/private goods",
- usage of cookies on the websites of the data controllers without observing, cumulatively, the provisions of Article 4 (5) letters a) and b) of Law no. 506/2004.

Section 3 The activity of solving complaints and notices

I. Overview

The purpose of adopting the Law no. 677/2001, as provided by Article 1, is to guarantee and protect the fundamental rights and freedoms of individuals, in particular the right to intimate, family and private life, in connection with the processing of personal data and the free movement of such data. In order to achieve this, one of the main attributions governed by law within the competence of the national supervisory Authority is to defend these rights and freedoms of individuals by solving complaints and notices concerning their infringements.

Thus, natural persons who consider themselves injured by the way their data are processed by data controllers or data processors can address complaints to the national supervisory Authority. The legislator also regulated the possibility for any person to refer the matter to the national supervisory Authority if he/she finds that some processing of personal data might be contrary to legal provisions.

In order for the complaints to be considered admissible, individuals must meet several conditions stipulated in the law: not to initiate a legal action with the same object and with the same parties; to forward previously (15 days) an application with the same content to the data controller, to which he/she has not received a response from the data controller or the response is not satisfactory.

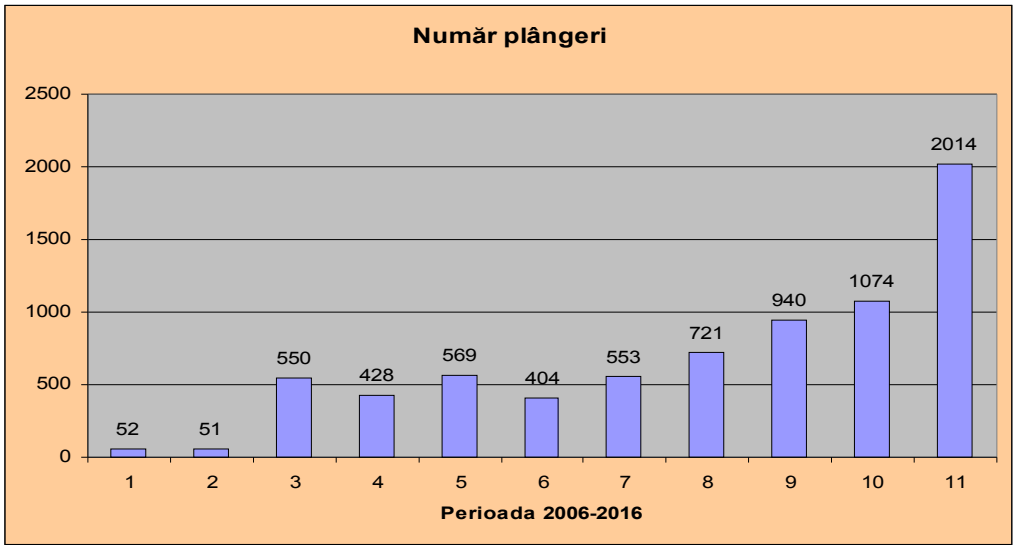
Thus, although one of the reasons for the rejection of the complaints was also in 2016 related to the failure of the petitioners to comply with the legal procedure, there was a considerable increase in the number of admissible complaints, which proves a better information to the data subjects on the conditions they have to comply with when submitting a complaint to the national supervisory Authority.

Among other reasons for which complaints and notices could not be retained in order for the authority to take action we may list: failure to provide evidence to substantiate the claims or the status of representative of the data subject (e.g. lack of legal empowerment or mandate issued in accordance with the applicable legal provisions); the notification of facts in relation to which the national supervisory Authority does not have the legal material competence (e.g. enforcement issues in the area of consumer rights or criminal law) or territorial one to intervene (e.g. processing carried out on the territory of another State); the impossibility of an accurate identification of the complained entity (e.g. unclear identification of the sender of an unsolicited commercial electronic communication or the owner of a website).

In 2016, the number of petitions handled by the specialized department of the national supervisory Authority almost doubled in comparison with 2015. Thus, a total of **2302 petitions** (compared to 1335 in 2015) were received and handles, out of which **2014 complaints and 188 notices**. From the content of petitions, it can be seen that this considerable increase in the number of petitions received in 2016 is the result of a better understanding of the legal powers of the national supervisory Authority by individuals compared to the previous period and of increasing the petitioners' confidence in the institution's actions for respecting their rights and freedoms.

Taking into account the exponential evolution of complaints from 2006-2016 (their number increased **more than 38 times** compared to the first year of activity), we consider it imperative to increase the number of staff of the national supervisory Authority involved in this activity, especially in view of the 2018 implementation of the new general regulation on the protection of personal data in all Member States of the European Union. According to the future legislative framework, any data subject will have the right to file a complaint with a supervisory authority, particularly in the Member State where he/she has his/her habitual residence, where his/her place of work is or where the alleged violation of the regulation took place.

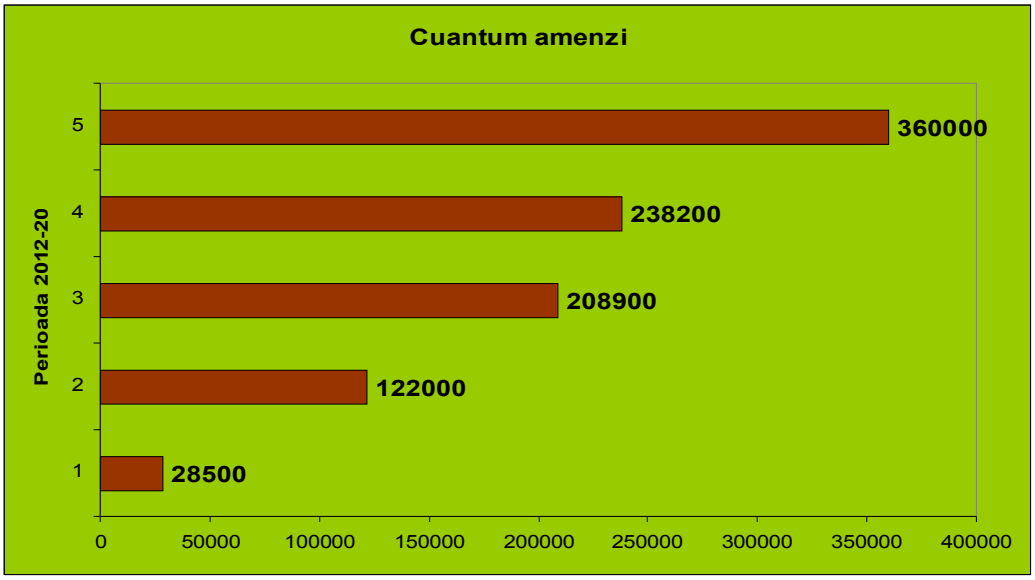
Figure 1: Number of the complaints for the period 2006-2016



In order to solve the complaints and notices received, **492 investigations were conducted**, out of which **202 on spot investigations and 290 written investigations**; **in 85 cases**, the investigations were finalized by concluding at the premises of the national

supervisory Authority the report of findings/sanctioning. Thus, compared to 2015, it can be seen that the activity of handling complaints/notices **has doubled**, and for the written investigations, the number of complaints/notices **has increased more than 4 times**. On the occasion of the investigations conducted for handling complaints and notices, contraventional sanctions were imposed, the total amount of fines applied in 2016 being **360,000 lei**.

Figure 2: The amount of the fines impose in the activity of handling complaints and notices for the period 2012-2016



At the same time, as a result of complaints and notices addressed to the authority, **8 decisions** of the president of the national supervisory Authority were issued requesting the deletion of personal data or of certain categories of data. The main areas in which these decisions were issued are related to reporting negative data to the credit bureau, monitoring condominiums through video surveillance and direct marketing.

Complaints and notices received during the year 2016 concerned a wide range of areas but, as in previous years, most of the complaints were referring to possible infringements of the right to the protection of personal data in connection with the granting of credit, the use of video surveillance systems, the transmission of commercial communications by electronic means of communication, the disclosure of data to various entities or the dissemination of data over the Internet. An issue that was reported in 2016, in many cases compared to the previous period, refers to the use of cookies on certain websites, without complying with legal requirements.

Regardless of the field of activity of the data controllers, many of the complaints received were related to the non-conpliance with the legal provisions concerning the exercise of the rights of the data subjects (in particular, right of information, right of access, right of intervention, right to oppose).

Concerning the processing of personal data related to the granting of credits, in 2016 there was an accentuated increase in the number of complaints filed in against banks, non-banking financial institutions or debt recovery companies. The main reasons for dissatisfaction of the data subjects were further determined by the non-observance of the provisions of Law no. 677/2001 and of the Decision of the national supervisory Authority no. 105/2007, which regulates the processing of personal data in the evidence system of credit bureau type systems.

A significant number of complaints and notices in 2016 referred to the processing of personal data by means of video surveillance, a matter regulated by the national supervisory Authority through Decision no. 52/2012 on the processing of personal data by means of video surveillance. The complained data controllers were mainly owners' associations, various categories of employers who installed a video surveillance system at the workplace, and individuals who installed video surveillance cameras that capture images from the public space. Personal data processing through video surveillance systems installed at the level of the educational units were also notified and investigated.

In 2016 a number of petitions have been submitted referring to the disclosure of personal data over the Internet without the consent of the data subjects or any other legal basis. The complained data controllers were companies that manage various social network websites, companies that have taken over and disseminated information from court files, as well as public authorities/institutions. Also, the national supervisory Authority continued to receive complaints in 2016 (in a smaller number compared to previous years) that concerned Google's failure to comply with the "right to be forgotten", as a result of the refusal of this company to respond to requests referring to the deletion of data indexed from the Internet from the search results associated with a person's name.

An important part was represented by the complaints through which the petitioners notified the national supervisory Authority about receiving unsolicited commercial messages by electronic means of communication. The complained data controllers were mainly companies engaged in online or direct marketing activities and electronic communications service providers.

Following investigations in 2016, although there has been a decrease in the number of cases where data controllers are unaware of the legal provisions applicable to data processing, further infringements of these provisions by data controllers have been identified as a result of non-compliance or failure to comply with obligations according to the law.

In the majority of investigated cases, the data controllers implemented the measures ordered by the national supervisory Authority (e.g. deletion of data unlawfully processed, deletion of results posted on the Internet, transmission of appropriate answers to persons who have exercised their rights provided by law etc.) in order to comply with the regulations in force in the field of personal data protection.

In order to inform the interested persons, both the complaints' templates and a detailed procedure on the conditions under which complaints and notices regarding possible infringements of Law no. 677/2001 or Law no. 506/2004 are available on the website of the national supervisory Authority.

II. The main findings from the activity of handling complaints and notices

1. Reporting personal data to an evidence system of credit bureau type

In 2016, the number of complaints relating to the transmission of personal data to the credit bureau increased considerably, occupying the first position as a share of the total number of petitions received by the national supervisory Authority. Generally, individuals who have submitted such a complaint have learned about the existence of negative data (delays in paying credit rates) in the credit bureau's evidence system when requesting other banking products, sometimes after several years after the data had been transmitted by the participants to this system. Therefore, the lack of prior, correct and complete information, a mandatory condition imposed by Decision no. 105/2007 in order for negative data to be reported by banks or non-banking financial institutions was the main reason why our institution was requested to intervene.

The high number of complaints received in this area has led to inquiries being made in most cases in writing, asking for clarification of the circumstances in which negative data was transmitted to the credit bureau for each of the particular complaint received. As a result of the investigations carried out, in many cases it was found that the conditions related to the

processing of personal data within the credit bureau were not respected, referring to: the type of information reported by the banks and the non-banking financial institutions, the way and the term for prior information required by the Law no. 677/2001 and Decision no. 105/2007, the term and frequency of reporting in a month. These findings indicate that the respective data controllers (participants in the credit bureau's accounting system) breached the provisions of Law no. 677/2001 and Decision no. 105/2007 which regulates their obligations regarding the transmission of the data of data subjects to the credit bureau.

In cases where, following the investigations carried out, it was found that the banks/non-banking financial institutions did not voluntarily respond to requests made by complainants or the recommendations made during these investigations, the national supervisory Authority ordered, by decision of the President, the deletion of data transmitted to the credit bureau without complying with the law.

CASE-LAW

Through several petitions, a petitioner reported a possible infringemente of the provisions of Law no. 677/2001 by a bank, which he/she claimed to have sent the data to the credit bureau without informing him/her in advance, in accordance with the provisions of Decision no. 105/2007.

The petitioner also claimed that the right of access, the right of intervention and the right to oppose under Law no. 677/2001 were infringed because the data controller did not handle his/her requests to exercise the abovementioned rights and did not reply within 15 days.

In order to solve the petition, an investigation was carried out at the bank and it was ascertained that, as the petitioner failed to pay his/her debt in due time, he/she was reported to the credit bureau with negative data, but by infringing the provisions of Article 12 of the Law no. 677/2001 and Article 8 of Decision 105/2007, namely without being able to prove the prior notification to the complainant prior to reporting. The bank also sent the petitioner a response to his/her request, without respecting his/her choice of sending the response to a specific email address, thus violating the provisions of Article 15 of Law no. 677/2001.

In this context, the bank was sanctioned for the contraventions provided by Article 32 of the Law no. 677/2001 with reference to Article 12 and 15 of the same law and Article 8 of

Decision 105/2007 and was recommended to delete the negative information reported to the credit bureau by breaching the legal provisions.

CASE-LAW

Through the petition, the petitioner complained that he/she was reported with negative data to the credit bureau in connection with a contract with a non-banking financial institution to issue a credit line although he/she was not notified 15 days before the date of the transmission of the data.

In the course of the investigation, the representatives of the financial company stated that, as the petitioner did not make monthly payments within the contractual maturity, he/she accumulated outstanding payments during the course of the credit and consequently sent his/her negative data to the credit bureau. However, the financial institution did not prove the prior information of the petitioner before the transmission of the negative data, as provided by Articles 8 and art. 9 of the Decision no. 105/2007, with the exception of two of the negative reports sent to the credit bureau.

The financial company did not respond to the request of the petitioner to erase his/her data from the Biroul de Credit's database, arguing that negative data was transmitted after the notification of at least 15 calendar days prior to reporting, but that aspect was not proven.

On the basis of these findings, the financial company was sanctioned according to Article 32 of the Law no. 677/2001 and Decision no. 105/2007 and it was informed about the obligation to delete the negative data transmitted to Biroul de Credit, without informing the petitioner in advance according to Articles 8 and 9 of Decision no. 105/2007.

CASE-LAW

Through the petition, the petitioner noticed a possible violation of the provisions of Law no. 677/2001 by a non-banking financial institution by the fact that he/she is reported with negative data to the credit bureau, although it was not notified 15 days before the date of their transmission of the outstanding payments recorded and the possibility of reporting them at the credit bureau.

During the investigation, the representatives of the financial company stated that as the petitioner did not pay the monthly installments due, they sent his/her negative data to the credit bureau. From the documents analyzed, it appeared that the notification of the petitioner for all reports made to the credit bureau according to Articles 8 and 9 of the Decision 105/2007 was not performed and in several cases such notifications were exceeding the 15-day term stipulated by the law; moreover, the prior notice did not contain precise information on the amounts due to be reported to the credit bureau.

On the basis of these findings, the financial company was sanctioned according to Article 32 of the Law no. 677/2001 and Decision no. 105/2007. At the same time, through the decision of the president of the national supervisory Authority is was ordered the deletion of the negative data transmitted to Biroul de Credit without the prior notification of the petitioner, as stipulated by Articles 8 and 9 of ANSPDCP Decision no. 105/2007.

2. Processing of personal data through video surveillance means

In this area, the petitions submitted to the national supervisory Authority continued to be significant as a result of individuals' awareness of their rights and of the role of the national supervisory Authority for the defence of these rights, in the context in which it is found that situations where different legal or natural persons decide to resort to the installation of video surveillance systems are becoming more common.

The processing of personal data through the use of video surveillance systems is subject to the provisions of Law no. 677/2001, as amended and supplemented, to those of the Decision of the national supervisory Authority no. 52/2012, as well as those of Law no. 333/2003 on the security of objectives, goods, valuables and the protection of individuals, as amended and supplemented.

The national supervisory Authority conducted a series of investigations concerning the processing of data through video surveillance systems installed at the level of public and private legal entities that installed such systems in the workplaces in order to monitor the activity of their own employees, but also installed by some school units as a result of the complaints and notices received, especially from some of the teachers working in the respective units. A significant part of the investigations in this area took place at the level of the owners'

associations where video surveillance cameras were installed in order to protect the condominium property and for the safety of the people living in the buildings.

In this context, Article 8 of the Decision no. 52/2012 sets out the cases in which the processing of personal data of employees by means of video surveillance is permitted, namely: for the fulfillment of express legal obligations or legitimate interest, by respecting the rights of the employees, especially their prior information. Paragraph (3) of the same article of Decision no. 52/2012 states that "the processing of employees' personal data using video surveillance inside the offices where they carry out their duties at the work place is forbidden, except for the cases expressly provided for by the law or with the notice given by the National Supervisory Authority for Personal Data Processing".

In view of the above legal provisions, the national supervisory Authority has taken the view that videosurveillance at the workplace can not be allowed in situations where there are far less intrusive means to achieve the declared goals (protection of goods or employees or monitoring the performance of their activity in terms of efficiency). At the same time, proof must be provided that the union or employee representatives have been consulted about the purposes for which the decision to install video surveillance cameras is being made, arguing that the personal data of the employees should be processed by these means. Also, throughout the operation of video surveillance systems it is necessary to provide permanent information, which is usually ensured by displaying representative icons near the monitored sites, accompanied by a series of information required by Decision no. 52/2012.

With regard to the installment of video surveillance cameras by individuals for their personal use (e.g. protection of privacy or private property), the national supervisory Authority has taken steps to investigate complaints or notifications received only if it considered that the legislation is applicable, i.e. in situations where individuals operate a video surveillance system installed on personal property that captures and stores images from the public space (according to the judgment of the Court of Justice of the European Union of 11 December 2014, delivered in František Ryneš v Úřad pro ochranu osobních údajů). In other situations, Article 2 (6) of the Law no. 677/2001 which concerns the exemption from the application of the provisions of the legislation on the protection of personal data in the case of data processing carried out by natural persons exclusively for their personal use if the data in question are not intended to be disclosed becomes incident. These provisions are reiterated by Article 17 (2) of the Decision no. 52/2012.

Following the investigations carried out to several categories of data controllers, in particular to owner's association, it was found that they do not have knowledge or do not comply with the provisions of Law no. 677/2001 and of Decision no. 52/2012. Due to the proliferation of condominium cameras installation, during the investigations conducted at the owners' associations, in order to better understand their obligations, the owner's associations' representatives have been informed about the Guidelines on processing personal data carried out by video surveillance systems installed within the owners' associations issued by the national supervisory Authority in 2014 (available on the authority's website).

CASE-LAW (owners' associations)

Through a petition filed with the national supervisory Authority, a natural person has reported a possible violation of legal provisions, meaning that the owners' association has installed a video surveillance system inside the building without complying with the applicable legal provisions.

As a result of the investigation, some of the claimed aspects were confirmed, so that the owners' association was sanctioned for the contraventions provided by Article 31 of Law no. 677/2001 (for the failure to notify the processing to the authority) and Article 32 by reference to Articles 12 and 4 of the same law (unlawful processing of personal data, as there was no adequate and complete information of the data subjects with regards to this processing, and the installation of cameras in elevators was considered to be excessive in relation to the stated purpose). At the same time, it was recommended to the association, inter alia, to cease processing the data of the data subjects (image) through the surveillance cameras installed in the elevators.

CASE-LAW (city halls)

Through the petition filed with the national supervisory Authority, a natural person reported a possible violation of the provisions of Law no. 677/2001 by the city hall of a commune, in the sense that it processes the personal data of its employees through a video surveillance system installed inside the mayor's office, including the offices, by illegally monitoring their activity.

As a result of the control, the territorial administrative unit (represented by the commune's mayor) was sanctioned for the facts provided by Article 31 of Law no. 677/2001

(failure to notify the processing to the national supervisory Authority), Article 32 with reference to Article 12 (not providing adequate information to the data subjects), Article 32 with reference to Article 4 (processing of personal data without complying with the legal provisions in force which prohibit the installation of video cameras in the employees' offices if there is no express legal obligation or an authorisation previously issued by the national supervisory Authority).

CASE-LAW (educational units)

Through a complaint addressed to the national supervisory Authority, a petitioner reported that a school infringed the provisions of Law no. 677/2001, in the sense that it has a video surveillance system that illegally processes images with students or teachers, provided that the surveillance cameras were installed inside the classroom as well.

During the inspection carried out in order to solve the complaint, the school motivated the installation of the video surveillance system as an obligation to supervise the operations carried out during the national evaluation exams through the video cameras installed in the examination rooms and in the offices where the subjects of the exam are multiplied (the director's office). However, it was found that, at the time of the investigation, the surveillance cameras in the classrooms were functional also outside the national evaluation exams, and it was ordered to keep the surveillance cameres in the classrooms only during the period exams and to delete the existing records outside of this period.

At the end of the investigation it was ascertained the contraventions provided by Article 31 of Law no. 677/2001 (failure to notify the data processing to the national supervisory Authority), Article 32 infringing Article 12 (unlawful processing of personal data as a result of the lack of information according to the legal provisions), as well as by Article 33 of the same law (failure to fulfill the obligations regarding the confidentiality and the enforcement of security measures, since the school did not adopt sufficient security measures to prevent unauthorized access or disclosure of images captured through the video surveillance system installed in school, which could be also accessed via the Internet, from the residence of the school director).

CASE-LAW

Through a complaint submitted to the national supervisory Authority, a former city mayor noticed the disclosure to third parties of images with him and his wife, caught by a surveillance camera installed in the city hall, the images being transmitted to the press.

During the inspection, the reported issues were confirmed. Thus, it was found that at the city hall level there was not developed and implemented a security policy for data processed through the video surveillance system, which would include the minimum security requirements for personal data processing and the information about the access files, personnel training, computer use, data printing, type of access, user identification and authentication, etc., according to the provisions of Order no. 52/2002, which also led to the unauthorized access and disclosure of the images collected by the surveillance system. As a result, a contravention sanction was applied on the basis of Article 33 of Law no. 677/2001, since no sufficient security measures have been adopted in order to prevent the unauthorized access or disclosure of images captured through the video surveillance system installed in the city hall.

It was also found that, although on each floor of the city hall icons were displayed, they did not contain all the information according to Article 12 of the Law no. 677/2001, and sanction was applied according to Article 32 of the Law no. 677/2001. Another sanction applied under Article 32 concerned the non-observance of the petitioner's right of access, since the city hall did not respond to his request.

3. Disclosure of personal data by different entities

Several complaints addressed to the national supervisory Authority have highlighted the infringement of legal provisions on the conditions under which personal data were disclosed to the general public (by publishing on websites, blogs, etc.) or to various public and private legal entities, without having previously obtained the consent of the data subjects or without informing them. Also, in some cases, investigations have revealed that the disclosure of personal data has taken place without a legal basis or in a disproportionate manner with reference to the purpose pursued.

Following the publication of personal data on various sites, they are subsequently indexed on the Internet by using search engines. Therefore, if that information is not relevant to the public interest, it is no longer up to date or is not correct, it is necessary to delete it; in

this respect, the data subjects can directly request search engines to respect the "right to be forgotten", as enshrined in European law and in the CJEU case law.

a) **"The right to be forgotten" on the Internet**

In 2016, the national supervisory Authority continued to register complaints (albeit in a smaller number than the previous period) referring to the disclosure of personal data on the Internet, subsequently indexed by search engines, in connection with the court proceedings, on various pages managed by private individuals or private entities, or in press articles published electronically. In the case of complaints considered admissible, investigations were carried out to solve the issues notified.

In most cases, the complained data controller was Google Inc. who did not respond to the petitioners' request for deleting the URLs of their personal data, on the grounds that the information is of public interest or would be disclosed by a "government agency". Following the request of the national supervisory Authority, the most of cases were settled in favour of the complainants.

When examining each complaint received in this area of interest, the national supervisory Authority has taken into account the arguments set out in the judgment of the Court of Justice of the European Union (CJEU) of 13th of May 2014 in Google Spain SL, Google Inc. against the Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12), as well as the guidelines laid down in the "Guidelines for the application of the judgment of the European Court of Justice on Google Spain and INC v Agencia Española de Proteccion by Datos (EDP) Mario Costeja Gonzales C-131/12", adopted by the Article 29 Working Group, which also includes the Romanian national supervisory Authority.

CASE-LAW

A petitioner noted that his personal data (image), associated with a series of false and defamatory information, was published on several websites (electronic press). The information considered to be false was related to alleged allegations of a virtual relationship between the petitioner and a female person who claimed to be a student and who would have sought help with obtaining a false diploma, accusations which later turned out to be be unreal, the

petitioner being recognized innocent by an ethics committee of the university where he is acting as teacher.

The petitioner addressed Google Inc. with the request to delete his personal data indexed on the Internet using this company's search engine. He received a response informing him that, with reference to some URLs related to his name, they are working on blocking them, and for other URLs, the request was not met because they include information of public interest.

Following the investigation carried out by the national supervisory Authority, the URLs where the petitioner's personal data can be found were not removed by Google Inc. from the search list, the data controller requesting in court the cancellation of the address by which our institution requested that the URL mentioned by the petitioner to be deleted.

As a result of the court's dismissal of Google Inc.'s complaint, the national supervisory Authority requested again the data controller to respond to the URL removal request. Consequently, Google Inc. has blocked the URLs mentioned by the petitioner.

b) Other cases

The national supervisory Authority has been notified through various complaints about the disclosure of personal data to other entities that did not have the right to own them, or the publication of information on the Internet without the consent of the data subject or any other legal basis; in some cases, the disclosure may even have the effect of causing image damage.

From the investigations made in 2016 it was found that in some cases the unlawful disclosure of personal data resulted from data controllers not implementing the necessary security and confidentiality measures in order to prevent the unauthorized access to data or the uncontrolled dissemination of data in the public space.

CASE-LAW

A petitioner has notified the national supervisory Authority about a possible infringement of the provisions of Law no. 677/2001 by disclosing on the Internet the e-mail addresses to a series of URLs associated with a website.

From the verification of the URLs indicated by the petitioner, more than 200 e-mail addresses associated with the website owned by a travel agency have been made available on the Internet.

As a result of the investigation, it was found that the travel agency collects personal data, including e-mail addresses, via contact and booking forms available on a tourist promotion site, filled in and sent by interested persons, as well as by subscribing to the "newsletter" of the company.

Following the checks made in the company's database, a significant part of the e-mail addresses disclosed on the Internet at the URLs mentioned in the petitioner's report were identified, the data controller being unable to provide reasons justifying the disclosure of email addresses on the website it manages.

Upon completion of the actions undertaken, the national supervisory Authority sanctioned the data controller based on Article 32 of the Law no. 677/2001 (unlawful processing of personal data), as it did not provide complete information to natural persons whose personal data are collected on the company's website, but also based on Article 33 of the same law, by failing to apply appropriate technical and organizational measures to protect personal data from unauthorized disclosure or access, in particular in the case of data transmission within a network, which led to the disclosure of e-mail addresses of subscribers from the company database. At the same time, it was ordered the removal from the public space (Internet) of e-mail addresses illegally disclosed.

CASE-LAW

A petitioner complained about an infringement of the legal provisions concerning the processing of her personal data from the professional file managed by a rural village hall, whose employee is, through their disclosure (employment contract, graduation diplomas, job description) on a social network (Facebook) during the 2016 local election campaign in which her husband has run for mayor.

The investigation revealed that, as a result of defamatory information published on Facebook by the petitioner's husband, the mayor of that date, a candidate for in continuation occupying this function, considered it necessary to contradict this allegations by publicly disclosing the conditions considered illegal for occupying this function by the petitioner, based on documents deemed to be false. In this respect, he asked the secretary of the village for the

professional file of the petitioner and photographed with his personal phone a series of documents, which he later posted on the Facebook account of an acquaintance.

Upon completion of the actions undertaken, the national supervisory Authority sanctioned the village, represented by the mayor, based on Article 32 of the Law no. 677/2001 (unlawful processing of personal data), for the failure of the complainant's right to oppose, as well as on Article 33 of the same law, as no security and confidentiality measures have been adopted to prevent unauthorized disclosure of the personal data administrated by the village hall where the petitioner was employed, which led to the disclosure of her personal data on Facebook.

Considering the findings of the investigation and having regard to the provisions of the Government Decision no. 432/2004 regarding the civil servants' professional file, according to which the National Agency of Civil Servants has the competence to sanction the photocopying and/or transmission of photocopies from the documents included in the professional file to third persons, the national supervisory Authority notified the said institution.

CASE-LAW

A petitioner informed us that a court (tribunal) had refused to comply with the request for his personal data no longer to be published on the court portal, as there is no procedure regulated that purpose.

During the investigation conducted in this case, the national supervisory Authority informed the data controller about the information provided by the Ministry of Justice about similar situations, according to which the content of the portal webpages is in the administration of the courts, the electronic archiving period is of 24 months and begins to run from the date of settlement of the dossier, according to the rules established for the use of the ECRIS system (file management system in court).

Following the national supervisory Authority's inquiries, the file containing the applicant's personal data, belonging to the complained court, did no longer appear on the court portal as a result of its archiving into the ECRIS system.

CASE-LAW

The national supervisory Authority was notified that a visible copy of a school and vocational guidance certificate issued by a County Resource and Educational Support Center

containing a personal data (name, surname, date of birth, place of birth, home and residence address, personal numeric code), health data ("somatic" type of disability/disability) and the surname and forenames of his/her parents was published on a Facebook account.

From the examinations carried out, it resulted that the document was posted by the parents committee of a class from the secondary school where the minor was enrolled.

In the course of the investigations carried out, the national supervisory Authority sanctioned the secondary school for the act provided by Article 33 of Law no. 677/2001 by failing to adopt security and confidentiality measures to prevent the unauthorized disclosure of an individual's personal data by photocopying and further disclosing a document containing his/her data and his/her parents' data by posting an document on a Facebook account by the chairman of the parent's committee of the class where the minor learnt. The national supervisory Authority has also sanctioned the latter for the disclosure of the minor's data on Facebook, by infringing the provisions of Article 5 of the Law no. 677/2001.

CASE-LAW

A petitioner has notified our institution that a public authority has published on its website a list of persons who have filed applications under Law no. 544/2001, containing the names and surnames of several natural persons, as well as lists of legal persons to whom sanctions for contravention have been applied.

As a result of the steps taken, it appeared that the documents in question were not published on the website of the complained public authority but on Google Drive by a ministry to which that information had been communicated.

According to the statements of the representatives of this ministry, it was considered that the respective information was of real interest to the civil society, for which it was decided to publish them on the Ministry's website, given its role and purpose, to increase the transparency and the level of information regarding the activity of state's institutions.

Upon completion of the actions undertaken, the national supervisory Authority sanctioned the ministry on the basis of Article 32 of the Law no. 677/2001 (unlawful processing of personal data), as it revealed, by publishing on the Internet, the personal data of the persons who filed applications under Law no. 544/2001 (respectively names and surname) and of the authorized natural persons to whom sanctioning measures have been applied, without having the data transformed into anonymous data, without the consent and informing the

persons whose personal data were disclosed. Following the actions of the national supervisory Authority, the ministry removed the personal data from the public space.

4. Unlawful processing of the personal identification number

From the practice of handling complaints and notices addressed to the national supervisory Authority during the year 2016, there are various situations of infringement of the provisions of Law no. 677/2001, regarding the observance of the principles of legality and proportionality in the decision to process certain personal data. Thus, some data controllers have chosen to process personal data (even those protected by special rules, such as personal identification number or biometric data) for the purposes for which the categories of data could be limited to what is strictly necessary. In conjunction with these aspects, it was also found that in some cases the data continued to be stored or processed after the expiry of the legal period, although they were no longer necessary, depending on the justification of their initial collection. Also, the national supervisory Authority, according to its consistent opinions, did not allow the processing of biometric data for the purpose of accessing the workplace or establishing the working hours, where the data controllers could have chosen less intrusive means for the private life of individuals.

Regarding the processing of the personal identification number, there were found cases in which it is mandatory for certain transactions (e.g. issuance of fiscal invoices, return of marketed products), by incorrectly invoking some legal provisions that would require such processing. In this context, the national supervisory Authority monitored the compliance with Article 8 of the Law no. 677/2001 and Decision no. 132/2011 on the conditions of processing the personal identification number and other personal data having a general applicability identification function.

CASE-LAW

The national supervisory Authority was notified through a petition with reference to the conditioning of the collection of the personal identification for the issuance of invoices for individuals, i.e. the purchase of a product.

As a result of the investigation, it was found that the company processed the personal identification number of natural persons for issuance of invoices, although in Article 155 of the

Fiscal Code, provision in force until the entry into force of the new Fiscal Code, as well as in Article 319 of the the new Fiscal Code, this personal data is not mentioned among the mandatory data to be filled in for issuing the fiscal invoice for natural persons (other than taxable persons or paying VAT).

Therefore, the processing of the personal identification number for issuance of the invoice was not carried out neither on the basis of a legal provision, nor on the freely given consent of the data subject, nor with the authorisation of the national supervisory Authority as provided by Article 8 of the Law no. 677/2001 and Article 2 of ANSPDCP Decision no. 132/2011.

Consequently, the data controller was sanctioned for the act provided by Article 32 of the Law no. 677/2001, as it processed the personal identification number of the data subjects, for the issuance of the fiscal invoices, without complying with the provisions of Article 8 of the Law no. 677/2001 and Article 2 of ANSPDCP Decision no. 132/2011; it was also recommended to take the necessary measures to cease the processing of the personal identification number for the purpose of issuing fiscal invoices.

5. Non-observance of the right to information, right of access, right of intervention and right to oppose

The observance of the data subjects' rights regulated by Law no. 677/2001, in particular the right to information (Article 12), right of access to data (Article 13), right of intervention upon data (Article 14) and right to oppose (Article 15), even if it represents an essential obligation of data controllers, constituted the subject of many complaints submitted to the national supervisory Authority in 2016.

Thus, as a result of the investigations carried out, it was found that data controller are either unaware of their obligations under the above mentioned legal regulations, or knowingly ignore them, or they send to data subjects incomplete answers and/or without observing the 15-day deadline stipulated by the law, or they have not adopted sufficient and efficient organizational measures to handle the requests addressed by the data subjects on the basis of the rights regulated by Law no. 677/2001.

At the same time, there has been an increase in the awareness of the data subjects about their rights under Law no. 677/2001, irrespective of the area in which their personal data were processed, which resulted in an increase in the number of petitions having this object.

Regarding the importance that data controllers have to grant to the right to information, irrespective of their status as a public or private entities, we reiterate that this was confirmed by the CJEU judgment of 1st of October 2015 in Smaranda Bara and others against the President of the House the National Health Insurance Fund and the National Agency for Fiscal Administration (ANAF) - (C-201/14), in the context of the transfer of taxpayers' personal data between these two institutions, based on a bilateral protocol.

CASE-LAW

By petition addressed to our institution, the petitioner complained that a data controller did not provide him/her with all the information required following the exercise of the right of access provided by Article 13 of the Law no. 677/2001, information requested in writing from this data controller through several requests.

In addition, the petitioner also complained that three of the data controller's replies were sent to him/her by e-mail, although he/she had explicitly requested that the answers to be communicated to him/her by ordinary mail, indicating the address to which it should be transmitted.

As a result of the checks carried out in the course of the investigation, it appeared that the applicant had concluded two service contracts with this data controller, one for a television service and one for Internet service, but the contact relationship between the parties had ceased prior to the requests sent to the data controller.

From the responses sent by the data controller to the petitioner, it appeared that the later had not received, according to the provisions of Article 13 of the Law no. 677/2001, all the information concerning the processing of his/her data and that the replies were not sent to the address indicated by him/her.

Compared to the findings, the data controller was sanctioned for committing the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data), with reference to the provisions of Article 13 of the law. It has also been recommended to the data controller to send a new response to the petitioner, communicating him/her the information requested and taking the steps in order to ensure that in the future it responds to requests by which individuals exercise their rights under the law no. 677/2001, observing the provisions of Articles 13, 14 and 15 of the same law.

CASE-LAW

În fapt, petentul a sesizat că este nemulțumit de răspunsul comunicat de un inspectorat județean de poliție, căruia i s-a adresat în 2015 cu solicitarea ca datele sale personale, referitoare la o măsură educativă dispusă în 1991 printr-o hotărâre judecătorească (dată la care petentul era minor), să fie şterse din evidenţele de cazier judiciar ale acestei instituții, să nu mai fie dezvăluite ori utilizate, iar terţii cărora le-au fost dezvăluite să fie notificaţi cu privire la măsurile adoptate.

The petitioner complained that he/she was not satisfied with the response sent by a county police inspectorate, to which he/she requested in 2015 for his/her personal data concerning an educational measure ordered in 1991 by a court order (when the applicant was minor) to be deleted from the criminal record of that institution, to be no longer disclosed or used and the third parties to whom it was disclosed should be notified of the measures taken.

Thus, the complainant claimed that his/her data had been processed and disclosed to third parties without complying with the law, the complained public institution submitting in 2012, as part of an administrative litigation, among other documents, also certain reports, thus rendering public details of his/her private life, which would have influenced an unfavorable decision to authorize the conduct of an activity. On this occasion, the petitioner noted that at that time he/she was included in the operative records of a criminal record with an educational measure that should have been erased because the retention period had expired. Moreover, through a 2012 address, it had been communicated to the petitioner that the educational measure applied to him/her had been deleted ex officio since 2008, and since 2011 his/her data have been deleted, including from the "operative records", based on IGPR Disposition no. 18/2011.

During the investigation, the data controller acknowledged that the applicant's data had been deleted from the operative records, not on the date of entry into force of the IGPR Disposition no. 18/2011, but later in 2012, when the petitioner filed an application for the issuance of a criminal record certificate, and in 2015 the date was permanently deleted from all its records.

At the same time, it emerged from the investigation that the data of the petitioner was communicated to the courts and the central structure under the subordination of which the complained data controller operated. Therefore, the data controller's declaration that the notification to third parties to whom the applicant's data was disclosed would be impossible and

would entail a disproportionate effort to the legitimate interest, that could be harmed, was not well justified.

Based on the findings, the data controller was sanctioned for committing the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data), with reference to the provisions of Article 14 of the law because it did not notify the third parties to whom the data of the petitioner had been disclosed regarding the deletion of his/her data from the criminal record and the operative records of the criminal record, nor did it communicate a full answer to his/her request, according to the request made in the petition from 2015.

The data controller was also recommended to send a full reply to the complainant informing him/her about the information requested, as well as notifying third parties to whom the data of the complainant was disclosed on the measures taken.

CASE-LAW

The complainant pointed out that he/she had asked a telephone company several times to delete his/her personal data, as there was no contract with the telephone operator, but the reply was not satisfactory.

From the examinations made during the investigation, it appeared that the complainant concluded a contract with the data controller in 2005 for the purpose of providing telephone services and subsequently two other contracts. Because during the payment of the first contract, he/she had outstanding payments, his/her data was sent to a debt recovery company. However, from the correspondence carried out by the complainant with this company it is clear that the file drawn up in his/her name appears to be closed in the 2007company's records, the debit being recovered.

With reference to these findings, the data controller was sanctioned for committing the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data) relating to Articles 13 and 14 of the law, as it did not provide the petitioner with the information requested in the petitions submitted and did not comply with the request to delete the data it processed, as the contract had ceased its effects on the date of the request and the debt had been recovered since 2007 .

The data controller was also recommended to send a full response to the petitioner, as well as to delete the data from its records.

CASE-LAW

The petitioner complained that a company did not delete her personal data, such as name, address, telephone number, which was on the company's website. It also pointed out that this company did not reply to the request requesting for the deletion of these data and did not cease their dissemination to third parties, as it radiated since 2009 from the Trade Registry the form of organization in which she carried out the activity at a given moment, namely PFA (authorized natural person), and with which the personal information published on the site was associated.

During the course of the investigations, the data controller did not comply with the requests of our institution and refused to disclose all information regarding the processing of personal data. As regards the petitioner's request, the data controller stated that it did not identify this correspondence in the records of the company, although the petition had been sent by mail with confirmation of receipt signed by the data controller and that it did not identify any information in the computer records referring to the petitioner, although these data existed on the company's website.

Since the documents submitted showed that the petitioner exercised her right of intervention upon the processing of data and the data controller did not respond to her request and did not send her an answer, it was sanctioned for committing the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data), with reference to Article 14 of the Law no. 677/2001.

The data controller was also sanctioned for committing the contravention provided by Article 34 of Law no. 677/2001 (refusal to provide information) because it did not provide all the information or documents requested by the national supervisory Authority, in the exercise of the investigative powers provided in Article 27 of the Law no. 677/2001.

CASE-LAW

The petitioner reported that he/she had asked a bank to delete his/her negative personal data reported to the credit bureau, but did not receive a response to his/her request.

From the information obtained during the investigation, it appeared that the data controller processed the petitioner's personal data as a result of the credit agreement with him/her. Subsequently, as the petitioner has incurred outstanding payment, he/she was

reported with negative data to the credit bureau. Having failed to fulfill its obligations under Law no. 677/2001 and Decision no. 105/2007 to the data subject, in the sense that it did not inform him/her in advance, the data controller was sanctioned for committing the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data), in connection with Article 12 of the same law and Article 9 of the Decision no. 105/2007. At the same time, the national supervisory Authority requested the data controller to delete the negative data transmitted to the credit bureau for the petitioner for which it could not provide evidence of prior information.

Also, since the verified documents revealed that the petitioner exercised the right to oppose against the processing of his/her data by the credit bureau through the petition addressed to the data controller and the data controller did not reply within 15 days of the date the request, the later was sanctioned for the contravention provided by Article 32 of the Law no. 677/2001 (unlawful processing of personal data), with reference to Article 15 of Law no. 677/2001.

6. Transmission of commercial communications through means of electronic communication

During 2016, the high number of complaints and notices concerning the receipt of unsolicited commercial communications by telephone (SMS) or e-mail was maintained. Most of them were related to privacy protection in electronic communications sector, by receiving unsolicited e-mail messages without the express and unambiguous consent of the recipient.

In order to solve complaints considered admissible, the national supervisory Authority conducted a series of investigations to verify the consent of the data subject to receive commercial messages on his/her e-mail address or SMS. In some investigated cases, it was found that the senders of the commercial messages did not comply with the legal provisions in terms of obtaining the prior consent and compliance with the data subjects' option of no longer receiving unsolicited commercial messages. Thus, in many cases, it was found that data controllers continued to send commercial messages even after the data subjects had exercised their right to oppose, one of the reasons being related to the failure to operate appropriate opt-in subscription mechanisms (double "opt-in") and unsubscription.

CASE-LAW

Through several petitions, a petitioner claimed that she had repeatedly received unsolicited commercial messages from several e-mail addresses promoting various tourism services, although she did not ask to receive such messages. By the same petition, the petitioner also stated that she addressed the e-mail adresses' owner but did not receive any response. As a result of the verifications made, it was found that all the commercial messages received by the petitioner came from the same data controller.

As a result of the investigation carried out to this company, it was found that during the period in which the petitioner received the commercial messages, the company carried out marketing activities by sending commercial communications to e-mail addresses collected in several ways (on-line on the company's website, through forms filled in during tourism fairs and by telephone). Regarding the commercial messages received by the petitioner, the company was unable to identify the source of the e-mail address of the petitioner, so it can not prove her express and prior consent to receive commercial communications by electronic means.

During the investigation, the company's representatives stated that they had not responded to the complainant's requests, but they deleted the e-mail address of the complainant at the date of receipt of the request.

On the basis of the findings, the data controller was subjected to contravention sanctions under Law no. 677/2001 and the Law no. 506/2004.

CASE-LAW

One petitioner complained that he/she received an unsolicited commercial message on his/her personal e-mail address, which did not contain the identification data of the sender. By the same petition, the petitioner also stated that he/she addressed the e-mail holder ("Data controller 1"), noting that he/she had not previously accessed the promoted site and did not subscribe to receive a "newsletter". By the sent message, the applicant asks for the source of his/her e-mail address and the reason for sending the "spam". The petitioner received a reply stating that the commercial message was sent by an online marketing company ("Data controller 2"). Subsequently, the petitioner asked for the name of the marketing company that sent the message, but the request was left unanswered.

As a result of the investigations carried out by the national supervisory Authority to the two data controllers, it revealed that Data controller 2 sent commercial messages using its own infrastructure and database for sending marketing e-mails on behalf of the Data controller 1.

The representative of Data controller 2 could not specify the source of the collection of the e-mail addresses from their own database (indicating, for example, the purchase of databases without further details) and stated that they did not obtain the consent of the holders of the e-mail addresses for processing their data and sending commercial communications via e-mail. These statements have also been maintained with respect to the data of the petitioner.

In view of the above, Data controller 2 was sanctioned contraventionally on the basis of Article 13 in connection with Article 12 of the Law no. 506/2004. At the same time, it was asked to delete all personal data, including e-mail addresses, collected and used without the prior consent of the owners for the purpose of sending commercial communications and to stop sending commercial communications by electronic means without the express and prior consent of the holders of the e-mail addresses.

CASE-LAW

A petitioner complained of receiving commercial messages on his/her e-mail address from a travel agency, although he/she did not agree to receive these messages. The complainant repeatedly asked the data controller for information about the purpose of the data processing, the data processed, the recipients to whom the data were or was disclosed, the source from which the data and the automated mechanisms used were processed, the rights to the processed data, by mentioning that he/she did not consent neither for receiving commercial communications nor for processing his/her personal data.

The petitioner received an answer from the company informing him/her that the e-mail addresses to which the company sends tourist services offers are found in the agency's database "as a result of subscribing to a newsletter or a partner-website, as a result of previous correspondence etc."; the petitioner was also informed that the only personal data held was his/her e-mail address, as well as the fact that he/she has the possibility to unsubscribe by replying to the received message or by accessing the unsubscribe button inside the message.

However, during the investigation, the data controller could not accurately state the source of collection of the petitioner's personal data. In the company's electronic database, the petitioner's e-mail address appears in the contact list as unsubscribed. Therefore, the company's representatives did not submit any evidence of prior obtaining of the petitioner's

express consent for the purpose of transmitting commercial communications to his/her e-mail address, in accordance with Article 12 of the Law no. 506/2004.

Also, from the verification of the company's website where the subscription could be made in order to receive a "newsletter", there was no full information regarding the processing of personal data, according to Article 12 of the Law no. 677/2001, in particular as regards the rights of the data subjects and the conditions for their exercise.

On the basis of the findings, the data controller was subjected to sanctions under Law no. 677/2001 (Article 32 referring to Article 12) and Law no. 506/2004 (Article 13 referring to Article 12).

CASE-LAW

Through the petitions filed with the national supervisory Authority, a petitioner reported that she had received several commercial messages on her personal e-mail address from multiple e-mail addresses.

The complainant has previously addressed to the owners of the addresses from whom she received the commercial messages asking for information about the source from where they received her e-mail address, the purpose of processing this address, and whether there are recipients to whom it was disclosed, but she did not receive an answer.

The national supervisory Authority initially took the steps towards a commercial company whose object of activity was, inter alia, to register the domain names involved in sending unsolicited messages.

Following the investigation, it was found that the domains from where the complained commercial messages were transmitted were acquired by that company on behalf of and for another data controller. Consequently, the investigation continued to that data controller who effectively administered the complained domains. The representative of this company acknowledged that he had sent e-mails to the petitioner's address without being able to prove obtaining her agreement.

Following the investigation, it was found that the company neither did obtain the consent of the complainant for the transmission of commercial messages nor did it formulate and send a response to the petitioner upon her request.

On the basis of the findings, the data controller was sanctioned under Law no. 677/2001 and Law no. 506/2004.

CASE-LAW

Several petitioners have claimed to receiving commercial communications via e-mail from various entities, using computer services made available by a particular company.

Following the investigation, it was found that the data controller made available to its customers (mainly commercial companies) a platform for the transmission of e-mail marketing messages. As a result, during the inspection, the representatives of the national supervisory Authority requested that they provide the necessary information to identify the clients and all the circumstances surrounding the sending of messages to the petitioners.

Since during the investigation the data controller did not submit any document, physical or electronic form, in order to support its statements and did not allow any verification in the computer systems used, which were the subject of the investigation, it was envisaged to submit the information and documents requested within the time limit set.

The complained data controller did not comply and consequently was sanctioned under Law no. 677/2001 for the refusal to provide the national supervisory Authority with the information and documents required by it in the exercise of its investigative duties.

It should be noted that, in the absence of information held by such companies or providers of electronic communications services, the national supervisory Authority is in some cases unable to identify the senders of commercial communications by means of electronic communication and to engage them accordingly in legal liability.

7. Infringement of the rules for the confidentiality and security of data processing

One of the basic obligations of personal data controllers under the relevant legislation refers to the adoption of measures for ensuring the security of the processing and compliance with privacy rules in order to prevent incidents such as unlawful disclosure of data, unauthorized access to data, loss or destruction of data etc.

In 2016, some of the complaints and notices addressed to the national supervisory Authority concerned either the disclosure of personal data to third parties or on the Internet or the unauthorized access to personal data without the consent of the data subjects or a legal basis as a result of the fact that the data controllers in question (local public authorities,

telephone service providers etc.) have not implemented efficient, technical or organizational internal procedures to prevent such problems.

CASE-LAW

A petitioner complained that the right to the personal data protection of 138 people had been violated by the city hall of a village, which posted the data on its own website. By accessing the indicated URL, it was found that several documents containing personal data of the inhabitants of the village, including sensitive data, namely the personal identification number and health data, were published. Also, collective ads issued under Artcile 44 (3) of the Fiscal Procedure Code, which included a large number of persons, mentioning the name, full address, number and date of issue of the summons or enforceable title were available.

According to the Order of the Minister of Public Finance no. 94/2006 on the approval of the model and the content of the forms and the instructions for their completion in order to carry out the procedure of communication of the fiscal administrative acts by means of advertising, the communication through advertising is done in the case when the fiscal administrative act could not be communicated by one of the communication means referred to in Article 44 (2) - (21) of the Government Ordinance no. 92/2003 on the Fiscal Procedure Code, republished, as subsequently amended and supplemented, normative acts in force on the date of publication of collective notices. The communication of the fiscal administrative act through advertising is done by simultaneously displaying at the headquarters of the issuing authority and on its website a notice stating that the fiscal administrative act was issued on behalf of the taxpayer. The ad will be retained for 15 days from the date of display. The collective advertisement model set out in Annex no. 1^{B} to this order includes: name, surname, taxpayer's name, fiscal domicile, name, number and the date of the fiscal administrative act. This model does not contain the taxpayers' personal identification number.

Also, the Constitutional Court, in its case law (Decisions 1288/2008, 667/2009, 536/2011), considered that "The interest of fiscal authorities in making the taxpayer aware of the existence of a fiscal liability that is owned by the state implies the need to communicate the administrative act in which it is recorded by means of which the taxpayer is effectively informed about the existence of fiscal obligations in its charge. As such, the legislator provided that fiscal administrative acts can be communicated through advertising even when the taxpayer's domicile is known. However, in this case, before using this method, it is necessary to strictly

observe the order provided in Article 44 (2) letters a) - c) of the Government Ordinance no. 92/2003, so that the communication through advertising to represent only a last and subsidiary way."

Therefore, the communication through Internet advertising is the last subsidiary way of communication of the fiscal administrative act, if other modalities stipulated by the Code of Fiscal Procedure Code were not possible, namely: remission to the taxpayer/authorised person, if it is ensured the receival of the administrative act by signature or postal mail, with registered letter with acknowledgment of receipt; by fax, e-mail or other electronic means of remote transmission, if it is ensured that the text of the fiscal administrative act and the confirmation of its receipt are provided and the taxpayer expressly requested this.

Following the consultation of the City Hall website, provisions for granting/terminating the monthly allowance granted under Law no. 448/2006 on the protection and promotion of the rights of persons with disabilities, where the name and surname, the personal identification number, the home address, as well as the mention that it is a person with disabilities were identified.

Also, the provisions for granting family allowance, based on the provisions of Article 23 of Law no. 277/2010 on the family support allowance, which included the name and surname, the personal identification number and the address of domicile were published.

As a result of the investigation, it was noted that the disclosure or publishing of personal data, in particular those expressly stated by Articles 8 and 9 of the Law no. 677/2001, even accidentally or through a technical error (as claimed by the city hall), represents an infringement of the provisions of Article 20 of the Law no. 677/2001, by not ensuring appropriate technical and organizational measures for the protection of personal data.

Therefore, upon completion of the undertaken actions, the national supervisory Authority applied to the village concerned, represented by the mayor, a contraventional sanction based on Article 33 of Law no. 677/2001, as it did not apply appropriate technical and organizational measures, according to Articles 19 and 20 of the Law no. 677/2001, for the protection of personal data against the disclosure on the Internet.

In the same time, it recommended the following to the data controller:

- to implement the necessary measures in order to avoid the publication of the personal identification number and health data of certain natural persons outside the applicable legal framework;

- to implement the necessary measures in order to observe the provisions of Code of fiscal procedure (contacting the taxpayer in advance), before using the last regulated way (Internet advertising);

- to delete from the website of the institution the documents that contain the name and surname, the personal identification number, the domicile address, as well as the mention that it is a person with disabilities;

- to adopt a security policy for the performed data processing, according to Articles 19 and 20 of Law no. 677/2001 and Ombudsman Order no. 52/2002, including the implementation of the measures necessary in order to prevent the disclosure of the personal data of the data subjects on the website of the institution in other situations that the ones stipulated by law.

CASE-LAW

A petitioner notified the national supervisory Authority that he signed a subscription agreement with a telephone company and subsequently an account on the company's website was created, without his consent and information, through which the wife had access to information on the petitioner's telephone conversations.

In order to create an user account, the petitioner claimed that his wife provided her personal email address (which does not belong to the petitioner) along with the petitioner's personal data (name, surname, CNP, contract number/invoice number).

Following the investigation, it was found that in the user account creation process it was necessary to provide more personal information based on the contract number and / or the invoice registration number. The Confirmation of account creation is done by sending a message to the e-mail address provided when it was created.

Upon completion of the actions undertaken, the national supervisory Authority sanctioned the telephone company on the basis of Article 13 for infringing Article 3 of the Law no. 506/2004, as amended, as the data controller has not taken appropriate technical and organizational measures to ensure the security of the processing of personal data and to ensure a level of security proportionate to the existing risk, ensuring that the personal data of the contract holders concluded with the company telephony can only be accessed by authorized persons and protect that personal data against unauthorized access to prevent the creation and access of a user account by a person other than the contract holder. The lack of such measures

led to the creation and access of a petitioner's account by another person who was not entitled to use and access this data.

8. The use of cookies without observing the legal conditions

In 2016, the national supervisory Authority received a series of notifications requesting verification of certain websites registered in Romania (websites belonging to hotel units, advertising agencies or recruitment agencies) from the perspective of compliance with legal terms of use of cookies. Through these cookies it is possible to create profiles of the Internet user, on the basis of which personalized advertising is subsequently addressed.

In the investigated cases, the reported aspects were confirmed and it was found that although they were using such files to collect information from users' equipment, the websites in question did not provide adequate information at the time of the first visit on the website so as to allow an informed consent, as provided by Law no. 506/2004.

CASA-LAW

Through a petition, the national supervisory Authority has been notified that a personal data is being illegally processed on a hotel website. In fact, the petitioner noticed that on the website, although cookies are used, nor information is available on their use, neither information about the processing of personal data, under the conditions in which the name and surname, the e-mail address and phone number are collected, data that is required to be provided when requesting a price offer or booking.

From the website verification, the claimed aspects were confirmed, namely the website is using 7 cookies on that particular website and 11 from other websites (at the time of the inspection); contact and booking forms were available on the website, mandatory requiring the name, e-mail address, telephone number, as well as the arrival/departure date, breakfast, room type and a subscription form to "newsletter" through which e-mail address is collected. However, the website did not contain information about personal data protection and cookie usage policy, nor data on the identity of the company managing this website.

From the verifications and the tests perfomed when concluding the minute of the investigation, it was ascertain that, independently from the option of the visitor to accept or not the cookies, the cookies information was stored on the terminal device of the user.

Therefore, the use of these cookies on the website does not observe cumulatively the conditions provided by Article 4 of Law no. 506/2004.

Upon completion of the steps taken, the national supervisory Authority sanctioned the data controller as follows:

- based on Article 13 with regard to Article 4 of Law no. 506/2004 because certain existing cookies on the website are stored on the devices of the users following the access to the websites, withour being necessary to obtain the express and prior consent of the users;

- based on Article 32 of Law no. 677/2001 (unlawful processing of personal data) because the website does not contain information on the processing of personal data collected includinv through the contact and booking form.

CASE-LAW

The national supervisory Authority has been notified that there is no information on the cookies policy on a company's website.

As a result of the investigation, it was found that when a website was accessed, no notice was displayed so that users of the website are informed of the cookies policy and to give their informed consent of their storage before browsing the website. Also, there is no document on the website that contains information about the cookies policy of the target people visiting the website.

Upon completion of the actions undertaken, the national supervisory Authority sanctioned the data controller on the basis of Article 13 with reference to Article 4 of Law no. 506/2004, as there was no information on the website for the targeted persons, respectively their users, according to the provisions of Article 12 of the Law no. 677/2001.

CHAPTER V
INTERNATIONAL AFFAIRS ACTIVITIES

Cooperation on European and international level is a strategic aspect requiring the involvement in all initiatives under development. Such cooperation can take place through participation in various forums, such as the Article 29 Working Group, the International Conference of Data Protection and Privacy Commissioners and the Spring Conference of the European Data Protection Authorities.

In this context, in 2016, following the adoption in May of Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) and Directive (EU) 2016/680 on the protection of personal data in specific activities carried out by law enforcement authorities (the Directive on police and judicial activities), the national supervisory Authority participated in the implementation of the legislative package in the field of personal data protection.

As member of Article 29 Working Group, the national supervisory Authority has been involved in the preparation of the new data protection framework that will enter into force throughout the EU as of 25th of May 2018. Thus, the national supervisory Authority, representing by its members, participated in 2016 in a series of meetings and various working groups at European level. These include:

- Article 29 Working Group (set up based on Article 29 of Directive 95/46/EC) which reunites all the European authorities and the European Data Protection Supervisor,
- Subgroups: BTLE, Cooperation, Enforcement, Financial Matters, Future of Privacy, International Transfers, Key provisions, Technology,

➢Consultative Committee of Convention 108 of Council of Europe (T-PD),

➢Joint Supervisory Body of Europol and Joint Supervisory Authority of Customs,

➢VIS Supervision Coordination Group, SIS II Supervision Coordination Group and Eurodac Supervision Coordination Group,

➢International Working Group on Data Protection in Telecommunications, dedicated to protection of personal data in the electronic communications sector,

➢Working Group on personal data protection within Police Cooperation Convention for Southeast Europe.

Article 29 Working Group

During 2016, the Article 29 Working Group expressed its position on fundamental issues such as the reform of the European regulatory framework (the General Data Protection Directive and the Directive on police and judicial activities), the EU-US Privacy Shield, the publication personal data to ensure transparency in the public sector, the ePrivacy Directive, thus establishing an effective protection of personal data at European level.

Thus, we mention the following documents that have been adopted either in the form of opinions or in the form of working documents or statements:

- 2016 action plan for the implementation of the General Data Protection Regulation – the action plact was designed for 2016 and aims to set the priorities of Article 29 Working Group on the preparation for the new legal framework, in particular the European Data Protection Board (EDPB);
- justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) – Article 29 Working Group has drawn upon the jurisprudence to identify the European Essential Guarantees that should be in place to make sure interferences do not go beyond what is necessary in a democratic society. These guarantees are primarily based on the jurisprudence of the CJEU and the ECtHR in cases related to the application of the rights to privacy and data protection in Europe. This means these guarantees in the first place apply in and to the Member States of the European Union and the Council of Europe when applying European or national legislation interfering with these rights. Article 29 Working Group underlines that the guarantees are based on the fundamental rights that apply to everyone,

notwithstanding their nationality. Following the assessment of the jurisprudence, Article 29 Working Group comes to the conclusion that the requirements can be summarised in four European Essential Guarantees: a) processing should be based on clear, precise and accessible rules; b) necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; c) an independent oversight mechanism should exist; d) effective remedies need to be available to the individual;

- EU-US Privacy Shield – the document offers an assessment of the proposal of decision of European Commission and its annexes constituting a new framework for transatlantic exchanges of personal data for commercial purposes, namely the EU-US Privacy Shield which seeks to replace the previous U.S. Safe Harbour invalidated by the Court of Justice of the European Union in October 2015, in the Schrems case. Article 29 Working Group noted certain improvements compared to the previous mechanism. In this context, we mention the increased transparency in relation to public access to data transferred under the Privacy Shield, either for national security or law enforcement purposes. The fact that all data transfers to the U.S. will henceforth be given the same protection is also welcomed; there are no specific legal provisions in place to give advantage to one tool or another. However, three major points of concern do remain, that in the view of the Article 29 Working Group will need to be addressed, namely: i) the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary; an essential element of EU data protection law is to ensure that data is kept for no longer than necessary to achieve the purpose for which the data were collected; ii) the continued collection of massive and indiscriminate data is not fully excluded; Article 29 Working Group has consistently held that such data collection is an unjustified interference with the fundamental rights of individuals; iii) the Ombudsperson mechanism; even though the this step of creating an additional redress and oversight mechanism for individuals is welcomed, concerns remain as to whether the Ombudsperson has sufficient powers to function effectively; both the powers and the position of the Ombudsperson need to be clarified in order to demonstrate that the role is truly independent and can offer an effective remedy to non-compliant data processing. Article 29 Working Group welcomes the improvements offered by the Privacy Shield and urges, in the same time, the European Commission to resolve the concerns

expressed, to identify appropriate solutions and to provide the requested clarifications of Article 29 Working Group;

- publication of personal data for transparency purposes in the public sector – the opinion explains how to apply the data protection principles to the processing and publication of personal data for transparency purposes in the public sector, in particular when related to anti-corruption measures and the management and prevention of conflicts of interest. The document does not seek to address what information should be available via access to public documents/freedom of information legislation of the EU member states, does not limit the availability of such public information in accordance with national legislation, nor does it cover the implementation of Regulation 45/2001 and Regulation 1049/20013 applicable to EU institutions and bodies. The aim of this opinion is to provide practical guidance, recommendations and best practice examples for Member States' legislators and competent institutions on how they can ensure that the right to data protection is respected whilst at the same time balancing and satisfying the legitimate public interest in transparency;
- the evaluation and review of the ePrivacy Directive (2002/58/EC) – the evolutions of the digital market, alongside the recent adoption of the General Data Protection Regulation calls for a thorough revision of the rules in Directive 2002/58/EC (the ePrivacy Directive). The revision of the ePrivacy Directive must lead to a regulatory system that is coherent and effective, and offers legal certainty as to what legal provisions apply in any particular situation. The ePrivacy Directive has, since 2002, provided a set of additional security and privacy measures with a particular focus on telephony and internet access providers. Article 1(2) of the ePrivacy Directive provides that this Directive was laid down to particularize and complement the Data Protection Directive 95/46/EC, which will be repealed by the GDPR when it will shall apply on the 28th of May 2018. Article 29 Working Group supports the recognition of the need to have specific rules for electronic communications in the EU. Thus, the new instrument would provide additional protection to the electronic communications of natural and legal persons. The revised ePrivacy Directive should keep the substance of existing provisions but make them more effective and workable in practice, by extending the scope of the rules on geolocation and traffic data to all

parties, while simultaneously introducing more precisely defined conditions that take the intrusiveness of the processing of communication data to the private life of users thoroughly into account.

Consultative Committee of Convention 108 of Council of Europe

In 2016, the activities carried out at the level of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, known as Convention 108, with the participation of the national supervisory Authority, concerned, first, the modernization of Convention 108, establishing the criteria to comply with personal data protection requirements in the context of automatic exchange of personal data for fiscal purposes, processing of passenger data (PNR data). As a result of the concerns about the responses to terrorist attacks and threats, in the year 2016, the Consultative Committee of Convention 108 adopted an Opinion on the Data protection implications of the processing of Passenger Name Records. Thus, given the implications for the right to data protection and the right to privacy that PNR measures might have, the text of the document underlines the importance of demonstrating and respecting the legality, proportionality and necessity of a PNR system, taking into account in particular on the following issues:

- transparent demonstration of the necessity and proportionality of the system in light of the legitimate aim pursued;
- accurate and strict definitions of the legitimate aim pursued are required and processing of PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes, or in exceptional cases, prevention of serious threats to the public);
- publicity of the competent public authorities;
- transmission of data via "push method" with a clear definition of the initial retention period and appropriate security measures;
- prohibition of the systematic transfer of sensitive data;
- limitation of the data mining to predefined risk indicators;
- legal and only necessary limitations to the rights of information, access, rectification and deletion of the individuals;
- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective administrative and judicial remedies for the individuals;
- independent and external oversight of the PNR system;
- periodic review of the PNR systems by the competent authorities.

VIS Supervision Coordination Group, SIS II Supervision Coordination Group, Eurodac Supervision Coordination Group

The data protection framework of the VIS consists of specific rules contained in the legal acts governing this system, namely Regulation (EC) 767/2008 of 9th of July 2008 and Council Decision 2008/633/JHA, which complement the provisions of the Charter of Fundamental Rights of the European Union, Directive 95/46/EC, Regulation (EC) 45/2001, Council Framework Decision 2008/977/JHA, Council of Europe Convention 108.

The activity of the VIS Supervision Coordination Group aimed, inter alia, at an analysis of the access to VIS data and the rights of the data subjects. Thus, based on the responses to the questionnaires sent to the data protection authorities, reports were drawn up on the authorities designated to have access to the VIS data, the purposes for which they can use the system and the rights of the data subjects.

Therefore, is absolutely necessary to ensure that the data subjects can effectively exercise their specific rights under the relevant legislation in the field of visa issuance where compliance with the legal framework is essential.

Following the analysis, the VIS Supervision Coordination Group issued recommendations such as:

- updating the consolidated list of competent authorities having access to the VIS published by the Commission;
- for the competent national authorities to develop and formally adopt internal policies regarding access to and use of VIS data as well as security and data protection policies encompassing VIS purposes;
- as regards the procedures in place to answer data subjects' requests to access, correct or delete their personal data stored in the system, the Member States are encouraged to adopt uniform maximum time limits for replying in writing to such requests.

With reference to the activity of SIS II Supervision Coordination Group, in 2016 joint model for inspecting SIS II alerts elaborated by the subgroup composed of members from Belgium, France, Malta, Lithuania and Romania was finalized.

The document is focused on legality issues, completing the data security document developed by the subgroup of IT experts, and is structured in two parts: i) specific questions about each alert; ii) general questions relevant to each alert, e.g. misuse of identity, data quality, data retention.

As far as the Eurodac system is concerned, this system was established by Council Regulation (EC) no 2725/2000 of 11th of December 2000 (Eurodac Regulation), which was supplemented by Council Regulation (EC) no. 407/2002 of 28th of February 2002. The texts of the two Regulations were repealed by Regulation (EU) no. 603/2013 of 26th of June 2013 (the Eurodac Reform Regulation), which became applicable on 20th of July 2015.

Taking into consideration the new Eurodac legal framework, the Eurodac Supervision Coordination Group established during its April 2016 meeting, as part of the Work Program 2015-2018, the adaptation of the Standardised Inspection Plan to the new legal requirements of the Reform Regulation. The review of the 2012 inspection plan was carried out by the representatives of the data protection authorities from Romania and UK.

The document in structured to serve as a tool to assist data protection authorities in carrying out their specific supervision competences (according to Article 30), as well as their mandatory annual audit (according to Article 32(2)) and of the inspection to Eurodac system. The document and its structure provide a reliable and common methodology for inspections of national EURODAC access points, also allowing for a better analysis and comparison of results following the verifications performed by the national data protection authorities.

Joint Supervisory Body Europol (JSB Europol)

JSB Europol – composed of representatives of the data protection authorities of the EU Member States, as well as representatives of the Council of the Union - represents the joint body for monitoring the way in which the police authorities comply with the legal provisions on personal data protection, within the specific cooperation activities of police authorities through the IT system provided by Europol.

On 11th of May 2016, the European Parliament and the Council adopted Regulation (EU) 2016/794[1] regulating the activities carried out at Europol level and replacing the Decisions

[1] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

previously adopted by the Council of the Union. The provisions of the new Europol Regulation will apply starting with the 1st of May 2017.

Thus, the framework within which data protection authorities could cooperate in this area also changed. JSB Europol will be replaced by a new Joint Supervisory Body - referred to as the Cooperation Council - from the date when the provisions of the new Europol Regulation will apply. The representatives of the data protection authorities of the EU Member States as well as those of the European Data Protection Supervisor (EDPS) will attend the meetings of this new cooperation body.

In view of the amendments brought to the normative framework, the activities of JSB Europol during 2016 focused on ensuring the most efficient transition of activities to the new form of cooperation established by Article 45 of the European Regulation, respectively the Cooperation Council. The main purpose is to ensure the continuity and consistency of the oversight activity provided by data protection authorities and the EDPS.

The new Joint Supervisory Body will take over the ongoing activities at the JSB Europol level and will try to avoid overlapping or "doubling" past exercises at the JSB Europol level.

International Working Group on Data Protection in Telecommunications

The debates during the meeting of International Working Group on Data Protection in Telecommunications in 2016 focused on topics such as the use of biometrics in electronic authentication, privacy issues in social networks, privacy issues in ICANN's "new generation registration directory service" (RDS), privacy and security in internet telephony (VoIP), privacy on e-learning platforms.

The discussions resulted in the adoption of the Working Paper on Privacy and Security in Internet Telephony (VoIP). Even if the technology being used by various companies differs, similar privacy and data protection risks remain and therefore the recommendations apply to all and the recommendations apply to all types of multi-media services, namely:

- VoIP service providers should inform customers about the privacy and security characteristics of the VoIP service(s) they offer;
- hardware and software manufactures should perform Privacy Impact Assessments and they should implement appropriate technical measures;
- VoIP providers should offer data portability;

- providers, software developers and hardware manufacturers that process traffic data shall respect the principle of purpose limitation.

Working Group on Data Protection within the Police Cooperation Convention for Southeast Europe (PCC SEE)

Based on conclusions of the 1st PCC SEE Data Protection Working Group meeting, the Friends-of-Chairmanship Subgroup on Data Protection set up, representing national data protection authorities and ministries of interior of Hungary, Macedonia, Moldova, Romania, the Montenegrin Chairmanship-In-Office, and the PCC SEE Secretariat conducted a joint analysis of the compilation of national answers to the questionnaire on the national application of the PCC SEE data protection provisions.

In this context, the Subgroup recommends that the practical implementation of information exchange within the PCC SEE framework is started as soon as possible in order to enhance the region's ability to tackle occurring threats to regional and wider European security. In the same time, the subgroup "Friends-of-Chairmanship" finds that with the PCC SEE a sufficient legal basis for cross-border exchange of information among the Contracting Parties is in place.

The 38th International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners first met in 1979 and has been the premier global forum for data protection authorities.

The Conference seeks to provide guidance and recommendations at international level in data protection and privacy, by connecting the efforts of privacy and data protection authorities from across the globe.

In 2016, the 38th International Conference of the national data protection authorities was organised by the Data Protection Authority from Morocco. Within the event, 5 resolutions were adopted, namely:

- adoption of an international competency framework on privacy education
- personal data protection competency framework for school students
- developing new metrics of data protection regulation
- human rights defenders

- international enforcement cooperation.

The spring Conference of the national authorities for the protection of personal data

The spring conference of the European authorities for the protection of personal data represents one of the most important annual meetings of all the commissioners on data protection from the EU Member States and from other European states.

During the 2016 event, organised the Data Protection Authority from Hungary, the agenda focused on three topics with the most actual European relevance, namely:

- the data protection perspective on the supervision of the national security bodies
- the reform of the European data protection legislation, namely the new tasks and duties for all the data protection authorities as provided by the General Data Protection Regulation and the Directive on police and justice
- the modernisation of Convention 108.

Within this event, two resolutions were adopted: resolution on the new framework of cooperation and resolution on the transborder flows of personal data.

Schengen evaluation missions

An important aspect of the activity of the national supervisory Authority at external level is represented by the participation in 2016 to the Schengen evaluation missions in the data protection field in Luxembourg, Italy and Malta.

Schengen missions refer to the evaluation and monitoring of the application of the Schengen acquis, i.e. the analysis of the implementation of personal data protection rules, thus ensuring that Member States apply Schengen rules effectively and in accordance with fundamental principles and norms. At the end of each evaluation mission, a report shall be prepared on the basis of the responses sent by the evaluated country to the standard questionnaire[2] and the information provided by the authorities of that country during the evaluation visit. That document contains, inter alia, the findings and assessments of the

[2] Article 9 of Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen

legislative framework, of the data protection authority, the assurance of the rights of the data subjects, international cooperation.

Legislative package on personal data protection

After more than 4 years of negotiations, 2016 was marked by the adoption by the European Parliament on 14th of April 2016 of the legislative package on personal data protection at European Union level, consisting of two legislative instruments: General Data Protection Regulation and the Directive laying down specific rules on the protection of personal data applicable to specific activities carried out by law enforcement authorities. Thus, the General Data Protection Regulation will replace Directive 95/46/EC, the current legal framework in the field of personal data protection, and its provisions will be directly applicable in all Member States of the Union, thus establishing a single set of rules in the entire European Union.

The regulation brings about a number of changes to the rules established more than two decades ago by Directive 95/46/EC, which were, in fact, the main objectives pursued by the European Commission when it proposed the first draft text in January 2012:

- **for the citizens** – the rights will be consolidated. The data subjects will be able to obtain additional information on how personal data is processed, in a clear, accessible, and understandable way. The right to be forgotten is strengthened and a new right – the right to data portability – is introduced, giving citizens a better control over their personal data. Also, special protection is provided for the privacy of minors;
- **for companies** – administrative formalities are simplified and there is the possibility to have an unique "interlocutor" for all the European data protection authorities. At the same time, a set of compliance tools, including, for example, the code of conduct, the certification mechanism, which can be tailored to the level of risks to the rights and freedoms of data subjects (through consultation with data protection authorities), is also available;
- **for the data protection authorities –** the intensification of the competences, including imposing coercitive measures and administrative fine up to 20 millions euros or up to 4% of the total worldwide annual turnover of a company. In the same time, the data protection authority have the possibility to adopt joint decisions, whether to issue recommendations on compliance with the legal framework or the application of a sanction, thus giving greater protection to individuals;

- **the cooperation between the data protection authorities shall be organized and shall include an European body – European Data Protection Board (EDPB)** will be responsible for mediating the disagreements between data protection authorities and for developing a set of "European" principles.

The provisions fo the general data protection Regulation shall be applicable starting with the 25th of May 2018.

Entry/Exit System – EES

In February 2013, the European Commission presented a proposal for a legislative package on Smart Borders in order to monitor the management of the external borders of Schengen area. The package was formed of 3 legislative proposals:

- proposal for a Regulation establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the Schengen area,
- proposal for a Regulation establishing a Registered Traveller Programme (RTP),
- proposal for a Regulation to amend the Schengen Borders Code[3].

Following the debates during the meetings organised at European level, the European Commission considered it necessary to improve and simplify the 2013 proposals. Thus, the European Commission decided the following: the revision of the 2013 proposal for a regulation on an Entry/Exit System (EES); the revision of the 2013 proposal to amend the Schengen Borders Code in order to integrate the technical changes resulting from the new proposal for a regulation setting out the Entry/Exit System; the withdrawal of the 2013 proposal for a Regulation on the establishment of the Registered Traveller Programme (RTP).

The scope of the new Entry/Exit System includes the border crossing points by all third-country nationals who visit the Schengen area for a short stay (maximum 90-days stay in any 180-days period) for both travelers with visa, visa-free or eventually visa-based travel.

Family members of EU citizens enjoying the right of free movement or of third-country nationals enjoying the same rights of free movement equivalent to those of EU citizens, as well as citizens who do not yet have a residence permit should be registered in the Entry/Exit System, but are not subject to short stays rules, and controls are performed in accordance with

[3] COM(2013) 95 FINAL, COM(2013) 97 FINAL and COM(2013) 96 FINAL.

Directive 2004/38/EC[4]. Family members who are in possession of a residence permit provided by Directive 2004/38/EC are excluded from the Entry/Exit System.

This system shall collect the data and register the entries and exists in order to facilitate the cross border of bona fide travelers, as well as for a better identification of the over-stay persons. Moreover, the system shall register the refusals for entry of third country nationals covered by the scope of the Regulation.

European Travel Information and Authorisation System (ETIAS)

In the European Commission of 14th of September 2016, "Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders"[5], the Commission confirmed the necessity to find a balance between mobility and security strenghten, thus facilitating the legal entry into the Schengen area without the need for a visa. Visa liberalisation has proved an important tool in building partnerships with third countries, including as a means of ensuring effective systems of return and readmission.

In this context, the European Commission launched a feasability study[6] for a European Travel Information and Authorisation System (ETIAS).

In this respect, we mention that ETIAS shall be an automated system, set up for the identification of any potential risks presented by a visa exempted traveller to the Schengen area and shall gather information on these travellers prior to the start of the travel, to allow for advance processing of the data.

Therefore, the main function of ETIAS would be to verify the information transmitted by third-country nationals exempt from visa requirements by means of an online application before

[4] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC.

[5] COM(2016) 602 final

[6] Feasability study for a European Travel Information and Authorisation System (ETIAS), final report; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf.

they arrive at the EU's external borders in order to determine whether they pose certain risks in the area of irregular migration, security or public health.

Privacy Shield EU-US

In February 2016 the European Commission published the Communication from the Commission to the European Parliament and the Council "Transatlantic Data Flows: Restoring Trust through Strong Safeguards"[7], a proposal for a decision on the adequacy of the protection provided and the anexxes which constitutes the new legal framework for the transatlantic exchange of personal data for commercial purposes: the EU-U.S. Privacy Shield which replaces the Safe Harbour Principles which were invalidated by the European Union Court of Justice on the 6th of October 2015 in Schrems Case[8].

The documentation published by the European Commission was subject to the assessment of the data protection authorities under the Article 29 Working Group and was finalised by the adoption of an opinion[9]. Thus, on one hand, the commercial activity of the Privacy Shield was analysed and, on the other hand, the safeguards established in connection with the derogations to the Privacy Shield principles for the purposes of national security and public interest.

In august 2016 the Commission Implementing Decision (EU) 2016/1250 of 12th ofJuly 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield was published in the Official Journal of the European Union.

According to this decision, the U.S. guarantees an adequate level of protection of personal data transferred from EU to organisations in U.S. based on the EU-U.S. Privacy Shield, under the condition that those entitites process personal data in compliance with a strong set of principles and safeguards for the protection of privacy and personal data which are equivalent to the ones in EU.

At the same time, in support of individuals, also in August 2016, the Citizen's Guide on the EU-US Privacy Shield was published on the European Commission's website[10].

[7] COM(2016)117 final, 29th of February 2016
[8] Case C-362/14 - Maximilian Schrems v. Data Protection Commissioner, 6th of October 2015
[9] Opinion 01/2016 (WP238)
[10] http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf

The Citizen's Guide offers general information about the EU-U.S. Privacy Shield and also presents, briefly, the obligations of the companies which are part of the EU-US Privacy Shield, as well as the rights of the data subjects with reference to the processing of personal data: the right to be informed, the right to access and correct your data as well as the right to lodge a complaint.

Thus, the Citizen's guide offers information concerning the way in which the data subject can lodge a complaint against a U.S. company which process personal data based on the EU-US Privacy Shield to the following entities: the U.S. company, the alternative dispute resolution body, the national data protection authority, U.S. Department of Commerce, U.S. Federal Trade Commission, Privacy Shield Panel.

CHAPTER VI

PERSONAL DATA PROCESSING SUPERVISION ACTIVITY

In 2016, the national supervisoty Authority handled **7445** requests from data controllers, represented by notification forms and requests through which they asked for the opinion or the clarification of some aspects related to the processing of personal data carried out by them.

6930 notifications concerning the processing of personal data were hadled, out of which 5480 carried out on the Romanian territory and 1450 data transfers abroad.

Out of the 1450 notifications with data transfers to entitites abroad, in 1205 transfers were declared to European Union, European Economic Area and third country states with adequate level of data protection recognised by the European Commission (including the United States of America, to entities that have adhered to the Privacy Shield principles), as well as transfers to third states carried out under Article 30 of the Law no. 677/2001, amended and completed.

At the same time, 245 data transfers abroad under Article 29 (4) of the Law no. 677/2001, amended and supplemented, based on standard clauses and Binding Corporate Rules were notified.

Following the assessment of the data transfers to third countries, 37 transfer authorisations were issued.

In the same time, 515 requests of data controllers on aspects concerning the dispositions of Law no. 677/2001, amended and completed, were analysed.

Section 1 – The activity of data processing registration

According to Law no. 677/2001, the notification represents the rule for declaring the data processing. Depending on the nature of the processing and the risks to privacy, the national supervisory Authority may exemptions from the notification obligation. Thus, taking into account the fact that certain processing operations are recurrent in the activity of a data controller, does not involve the processing of sensitive data or are provided as legal obligations on the basis of normative acts, the president of the national supervisory Authority issued Decision no. 200/2015 on the determination of cases of processing of personal data for which no notification is required, as well as the amendment and repeal of decisions, which entered into force on 28th of December 2015.

This act was issued for the application of Article 22 (9) of Law no. 677/2001, according to which the national supervisory Authority may establish cases of processing for which the notification is not required. Moreover, is was taken into account the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC concerning the elimination of data controllers' obligation to notify the national supervisory authorities about the data processing carried out.

Subject to the provisions of Decision 200/2015, the national supervisory Authority has recorded in the Personal Data Processing Register mainly the following data processing:

- personal data processing that allows the geographical location of individuals by means of electronic communications (monitoring/security of persons and/or public/private goods by using the GPS);
- personal data processing by electronic means, with the purpose of monitoring and/or evaluating some personality aspects such as professional competence, credibility, behaviour or others (creating and using profiles of targeted persons for

the transmission of newsletters, reporting the violation of codes of conduct in the private environment – whistleblowing);

- personal data processing of minors through the Internet or electronic messaging (publication of results at various school and extra-curricular competitions, posting of pictures from school camps);
- personal data processing by means of video surveillance for the purpose of monitoring/security of persons/premises and/or public/private assets.

Regarding the use of the GPS geolocation system, the national supervisory Authority considered that this is a way of processing personal data as it allows the employer to identify an employee indirectly by locating the vehicle used by his employee even if the main purpose of processing is that of protecting the property of the company from possible theft.

In the same time, many data controllers, particularly from the private environment, have notified the national supervisory Authority of the processing carried out in order to monitor their employees by video surveillance.

Regarding the video surveillance of employees, the national supervisory Authority pointed out that the implementation of a video surveillance system could affect employees' rights, so that, in addition to the provisions of Law no. 677/2001, as amended and supplemented and Article 8 of the Decision no. 52/2012, the provisions of the Labor Code must also be observed. In this respect, prior to the implementation of such a system, a thorough justification for taking this measure is required, at the same time as the consultation with the trade union or employee representatives.

In addition, the real estate, hotel, utility providers and self-employed entities, licensed under a special law (bailiffs' offices, mediators' offices, law firms, individual medical practices), have notified the national supervisory Authority of the processing they carry out for the purpose of fulfilling their legal duties.

The national supervisory Authority has informed these entities that they have the quality of data controller and, implicitly, the obligation to comply with the data protection legislation, in particular the provisions of Articles 12, 19 and 20 of Law no. 677/2001, amended and supplemented, but are exempted from the obligation to notify.

Thus, the exemption from the obligation to notify the national supervisory Authority does not exonerate the data controllers from fulfilling their other obligations under the applicable legal provisions in the field of personal data protection (e.g. informing the data subjects under

the conditions stipulated in Article 12 of the Law no. 677/2001 and the implementation of appropriate measures to ensure the security of the data processing according to the provisions of Article 20 (1) of the same act and the minimum requirements approved by Order no. 52/2002).

Following the analysis of the notification forms, it was proposed to conduct **ex-officio investigations** to verify certain aspects of the processing of personal data, namely:

- clarifying the conditions under which the processing of minors' data is carried out within the activities specific to "advertising, marketing and publicity";
- verification of the conditions of processing data related to offenses, criminal convictions/safety measures or administrative or contravention sanctions for the risk management of the reputation of data controller's clients; preventing or correcting the current or future risk of negatively affecting the value of the assets and reputation of the controller's clients as a result of the unfavorable perception of counterparts, shareholders, investors or supervisory authorities about their image;
- control of conditions for the processing of data revealing racial or ethnic origin, political opinions, philosophical beliefs, trade union membership, political party membership, data concerning health, genetic data, biometric data, data concerning the sex life, data related to criminal convictions for organising a casting;
- checking the conditions for processing the personal identification number for marketing activities;
- verification of the way of processing biometric data (fingerprints) for human resources purposes, i.e. the record of the working hours of the employees;
- clarifying the conditions under which data processing is performed through a video surveillance system capable of performing facial recognition;
- verification of the conditions of processing personal data of persons by video surveillance means as well as of the recording equipment for telephone conversations;
- controlling the conditions for the processing of employees' biometric data and data on concerning health for the purpose of scientific research;

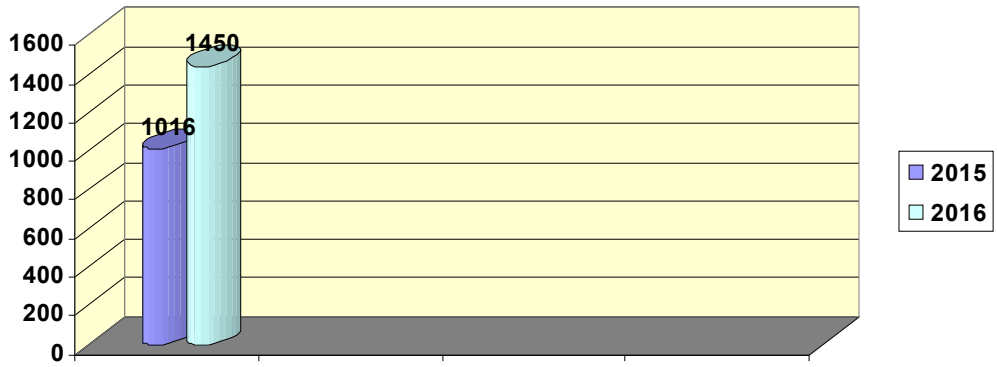
- verification of the conditions in which visitors' biometric data - facial recognition - is processed.

Section 2 – The transfer of personal data abroad

Regarding the transfer of personal data abroad, please note that according to Article 2 (1) of Decision no. 200/2015, it is no longer necessary to notify the transfer of personal data to European Union Member State, European Economic Area states, as well as to countries for which the European Commission has recognised, by decision, an adequate level of protection.

In 2016, the number of notifications with data transfers to foreign entities increased considerably compared to previous years. The increase in the number of notifications with the transfer of data abroad proves that data controllers know better their obligations according to the provisions of Law no. 677/2001.

Of the 1450 notifications with data transfers to entities abroad, in 1205 transfers were declared to European Union, European Economic Area and third country states with adequate level of data protection recognised by the European Commission (including the United States of America, to entities that have adhered to the Privacy Shield principles) as well as transfers to third States made under Article 30 of the Law no. 677/2001, amended and completed.



At the same time, 245 data transfers abroad were notified under Article 29 (4) of the Law no. 677/2001, modified and completed, on the basis of contracts with standard clauses and Binding Corporate Rules. Compared to previous year, we find that the number of personal data transfers performed on the basis of the above mentioned guarantees has doubled.

Among the areas that targeted data transfers to third countries, based on the provisions of Article 29 4 of Law no. 677/2001, as amended and supplemented, we mention the following:

- economic-financial and administrative management;
- management of clinical and non-clinical studies - processing the personal data concerning health of professionals, consultants, collaborators, freelancers involved in clinical trials;
- human resources and data management related to the recruitment, evaluation and promotion of staff;
- solving compliance complaints formulated by any interested person with respect to violations of the law, corruption offenses, service offenses, disciplinary misconduct, contraventions; ensuring compliance with applicable laws, principles, and internal regulations; uniformity of principles and regulations in order to carry out the activity according to the law at the level of the group;
- advertising, marketing and publicity and IT support, outsourced in case of incidents, problem support and IT support for IT systems;
- the use of electronic vouchers, i.e. the provision of specialised software to support card issuance and acceptance, authorization, reimbursement and processing of transactions;
- administration of benefit and incentive programs for employees;
- sponsorship, donations and loans; contributions to event costs, including registration fees, travel and accommodation costs.

Following the assessment of data transfers to third countries, 37 transfer authorizations were issued.

Section 3 – Opinions on data controllers' activity

During 2016, the data controllers and data subjects have requested from the national supervisory Authority various points of view regarding the legal conditions for the processing of personal data and the obligation to declare the processing carried out in relation to the provisions of Decision no. 200/2015. Here are some significant cases that are subject to the analysis of the National Supervisory Authority:

1) A representative of a legal entity has requested the national supervisory Authority to be notified with the necessary notification procedures for the implementation of an electronic system for establishing the working hours based on measurements/scans of employees' fingerprints.

In the context of this request, the data controller was informed that fingerprints (biometric data) are personal data as they relate to the physical/physiological characteristics of the persons and can lead to their identification, and their processing falls under the provisions of Law no. 677/2001, amended and completed.

The data controller was also informed that, according to Article 4 (1) of the abovementioned law, personal data intended to be processed must be processed in good faith and in accordance with the legal provisions in force, collected for specified, explicit and

legitimate purposes, the personal data should be appropriate, relevant and not excessive in relation to the purpose for which they are collected and further processed.

The national supervisory Authority considered that the employer should identify alternative solutions that have a lower impact on the employees' private life, considering the processing of biometric data as excessive in relation to the purpose pursued, in the context of the need to ensure an effective protection of the right to intimate, family and private life.

2) A legal person has requested the national supervisory Authority's point of view on the need to notify data processing in the context of the implementation of a portal within the companies it owns through which it is possible to notify the misconduct identified in the course of the activity (such as anti-competitive behaviour, safety at work, safety of information related to work techniques and company know-how) as a way of reporting subsidiary irregularities.

The portal will allow employees, business partners and stakeholders across the globe to report serious violations of conduct, violations of legal provisions and internal guidelines.

The national supervisory Authority has stated that the processing under discussion is in the situation regulated by Article 1 (1) letter e) of Decision no. 200/2015.

It was therefore communicated that in order to obtain the registration in the Electronic Register of personal data processing, it is necessary to fill in the on-line form for the general notification provided in the Annex to the Decision of the President of the NATIONAL SUPERVISORY Authority for Personal Data Processing no. 95/2008 regarding the establishment of the standard form of the notifications provided by the Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, published in the Official Journal of Romania no. 876 of 24th of December 2008.

3) A legal person has requested the opinion of the national supervisory Authority on the need for notification of the transfer of data to European Union countries, the European Economic Area, as well as to states for which the European Commission has recognised, by decision, an adequate level of protection.

Thus, it was stated that, according to Article 2 (1) of Decision no. 200/2015 issued by the President of the national supervisory Authority, "the transfer of personal data to coutries outside the European Union, outside the European Economic Area and countries for which the European Commission Union has recognised, by decision, an adequate level of protection,

including in the cases provided for in Article 1 is subject to notification of the National Supervisory Authority for Personal Data Processing".

It has therefore been mentioned that it is not necessary to notify the transfer of personal data to European Union Member States, the European Economic Area countries, as well as to countries for which the European Commission has recognised, by decision, an adequate level of protection.

4) A public institution has requested the opinion of the national supervisory Authority on the need to notify data processing for the issuance of property titles and on the conditions under which data may be disclosed to public authorities.

Regarding the subject under discussion, the national supervisory Authority has stated that, given that the processing operations to which it refers are carried out on the basis of legal provisions, the provisions of Article 1 (2) of the aforementioned decision, according to which "the notification is not necessary when the processing is provided for by law" are applicable.

In this context, where data of the nature of the ones shown in the provisions of Article 1 are not processed or if processing is provided by law, it is no longer necessary to fill in the notification form.

Regarding the disclosure of the data, it was mentioned that the rule established by Law no. 677/2001, as amended and supplemented, is that the processing, including the disclosure of the personal data of the data subject, may be performed by a data controller only with the expressed and unequivocal consent of the data subject. Also, Article 5 (2) of the aforementioned law expressly establishes certain exceptions from the obligation to obtain the consent in the case of the processing of personal data and, implicitly, of their disclosure by means of transmission, dissemination or in any other way.

5) A data controller has requested the view of the national supervisory Authority on the necessity to declare the processing carried out by means of an application which allows the use of a video channel for employment interviews within the recruitment process.

The national supervisory Authority has considered that the processing under discussion is in the situation regulated by Article 1 (1) letter e) of Decision no. 200/2015 and it is necessary to declare the processing carried out through the respective application.

6) A legal person has requested the national supervisory Authority's opinion on the legal conditions to be met in the case of video surveillance of employees.

In this respect, it was stated that the implementation of a system of video surveillance of employees could affect their rights, so that, in addition to the provisions of Law no. 677/2001, as amended and supplemented, and of Article 8 of the Decision no. 52/2012, the provisions of the Labor Code must also be observed. In this respect, prior to the implementation of such a system, it is necessary to justify taking this measure and, at the same time, to consult the trade union or the employees' representatives.

Decision no. 52/2012 establishes through Article 8 the situations in which the processing of personal data of employees through video surveillance is allowed, namely: for the fulfillment of express legal obligations or foor a legitimate interest, by respecting the rights of the employed persons, especially their prior information.

In addition to the above, the processing of personal data of employees by means of video surveillance can be done on the basis of their express and free-given consent, by respecting the rights of the employed persons, in particular their prior information.

At the same time, it was stated that, insofar as it is intended to extend video surveillance within the offices where employees work, this is allowed only in situations expressly provided by law or on the basis of the approval of the National Supervisory Authority for Data Processing Personal Character (Article 8 (3) of Decision No 52/2012).

Therefore, the rule of video surveillance within the offices is the prohibition of such processing, the exceptions being those expressly provided in a normative act obliging the employer to set up video surveillance systems or those authorized by the national supervisory Authority, according to Article 8 (3) of the Decision no. 52/2012, in duly justified cases.

It was also mentioned that the company in question has the quality of a data controller, meaning that it has the obligation to submit the notification.

7) An individual has requested the point of view of the national supervisory Authority with regard to the processing of personal data by means of video surveillance.

The individual was informed that the processing of personal data through the use of closed-circuit television systems with possibilities for recording and storing images and data is subject to the provisions of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as amended and

supplemented, of the provisions of Decision no. 52/2012 on the processing of personal data through the use of video surveillance means, with subsequent modifications and completions, as well as those of Law no. 333/2003 on the security of objectives, goods, valuables and the protection of individuals, modified and completed.

However, in accordance with the provisions of Article 2 (6) of the Law no. 677/2001, this act does not apply to the processing of personal data carried out by natural persons exclusively for their personal use, if the data in question are not intended to be disclosed.

At the same time, according to Article 17 (2) of the Decision no. 52/2012, the provisions of this decision do not apply to the processing of personal data by means of video surveillance performed by natural persons solely for their personal use if the data in question are not intended to be disclosed.

Therefore, a natural person does not have the quality of a data controller and is not required to notify the data processing (i.e. images recorded by video surveillance) to the national supervisory Authority if the images are used by the natural person only for personal use and disclosed to authorities with special investigative powers (for example, authorities with legal powers to investigate offenses).

However, to the extent that a natural person uses a video surveillance system that also captures images from the public domain, it has the quality of a data controller and, consequently, is subject to all the obligations as set out by Law no. 677/2001, with the exception of the notification of the processing to the national supervisory Authority, as provided in Article 5 of the Decision no. 200/2015 on the determination of cases of processing of personal data for which no notification is required, as well as for the modification and repeal of certain decisions.

8) The national supervisory Authority has been asked for a point of view on the obligations of data controllers that transfer personal data to the United States, based on the Privacy Shield certification with regard to the notification, in connection with Decision no. 200/2015.

In the context of the request submitted, the data controller was informed that, if the importer of data adhered to the Privacy Shield principles, the provisions of Article 2 (1) of Decision no. 200/2015 are applicable.

As a concequence, data controllers that transfer personal data to the United States based on the Privacy Shield certification are not under the obligation to notify the national supervisory Authority.

9) An institution responsible for setting up and organizing book collections and other library documents has informed the national supervisory Authority that it provides subscriptions to employees of commercial companies. In this context, the above mentioned institution received requests from the human resources department of the client companies regarding the behaviour and habits of the subscribers, the employees of the respective companies (what, how and when a subscriber reads, the title of the books, the number of the loans and loan date).

The national supervisory Authority considered that providing information related to the monitoring of the reader's behaviour is a processing of personal data that circumscribes the provisions of Article 1 (1) letter e) of Decision no. 200/2015, thus requiring to be declared, to the extent that is carried out electronically, and obtaining the reader's consent to disclose data about their behaviour.

CHAPTER VII

THE ECONOMIC MANAGEMENT OF THE AUTHORITY

In order to carry out its activity in 2016, the National Supervisory Authority for Personal Data Processing was allocated funds through the Law on State Budget no. 339/2015 and Government Ordinances no. 14 and no. 86/2016 regarding the rectification of the state budget for 2016, resulting in a final budget amounting to 4,851,000 lei, with the following structure:

- Thousands lei -

Indicator's name	Code	Initial budget 2016	Updated budget 31.12.2016	Amounts spent until 31.12.2016	Execution (%)
Total expenditures	51.01	3.256	4.851	4.767	98
Employees expenditures	10	2.485	3.727	3.721	99
Goods and services	20	750	765	688	89
Capital expenditures	71	21	359	358	99

As budget adjustments took place during the budget year, the priorities for the most important projects with the existing funds were constantly updated.

The approved final credits ensured the achievement of the proposed objectives, by taking into account the permanent demands for the efficiency of the use of public funds.

Regarding the way in which the funds are allocated, we can state that the amount of the national supervisory Authority's staff costs amounted to 76% of the total appropriations allocated from the state budget, from which credits were actually used worth of 3,720,823 lei (by occupying the posts, temporarily, by detachment), with a further major staff shortage (9 vacant posts, 5 posts temporarily occupied by detachment, representing 28% of the total

number of 50 posts - exclusively dignitaries - provided by Law 102/2005). Most staff costs were related to payments made for employees' salary.

The expenditures related to Goods and Services Title in 2016 had a 15% weight in the institution's budget and among these, the most important expenditures were:

- 12.95% expenses for internal travel due to the increased number of complaints and, implicitly, of the controls carried out at the data controllers in the territory, as well as the external travel to European working groups and subgroups, in the context of the European legislative changes
- 14% rental costs and 24% expenses on utilities and services provided by RA-APPS through SAIFI.

It should be mentioned that the national supervisory Authority has its main objective of activity through investigations and inspections to data controllers located on the Romanian territory, as well as to Romanian consulates.

At European Union level, the national supervisory Authority has the obligation to participate in the work of the Article 29 Working Party, its working subgroups, the meetings of the Coordinated Supervision Groups (SIS II, VIS, Eurodac) and the work of the Consultative Committee of Convention 108.

In 2016, the expenses on goods and services increased by 9% compared to 2015, with many factors being constantly under consideration - the expense opportunity, the lowest price criterion applied in public procurement procedures, along with carefully defined technical requirements.

As far as capital expenditure is concerned, the national supervisory Authority started in 2016 a project for IT infrastructure renewal, with a new server and storage system being purchased for them and licenses for the operation of servers and computers in the patrimony the institution, by using 63% of the amounts allocated to investment expenses.

The fleet of the institution was partially renewed through the PSIPAN 2016 program, by using 47% of the funds provided in the final budget of the Capital Expenditures heading.

It should be noted that the replaced fixed assets were purchased from the first budget allocated after the establishment of the institution in 2006.

The accounting policies used in the preparation of the annual financial statements are in accordance with the legal regulations in force.

The annual financial statements offer a true picture of the reality of the financial position of the institution, the budgetary allocations allocated to groups, titles, articles and expenditure items as set out in the Authority's budget.

The budget expenditures have been made in accordance with the principles of legality, timeliness, continuity and efficiency.

All documents that are subject to our own preventive financial control are verified and approved.

As a conclusion on the management of the allocated budget funds, we can say that they have been used with the utmost efficiency and careful management by our institution.