THE NATIONAL SUPERVISORY AUTHORITY FOR PERSONAL DATA PROCESSING

ANNUAL REPORT

2008

The activity report is presented to the Senate of Romania by virtue of art. 5 in Law no. 102/2005 regarding the establishment, the organization and the operation of the National Supervisory Authority for Personal Data Processing, published in the Official Gazzette of Romania no. 391 of May 9th, 2005, amended and supplemented.

Bucharest

FOREWORD

Mr. President of the Senate,

Dear Senators,

I'd like to present the report on the activity developed by the National Supervisory Authority for Personal Data Processing in its third year of existence -2008 .

The present report dwells upon some specific aspects of data protection we experienced both locally and during international reunions.

During the aforementioned year, our institution focused on two main courses of action: check the lawfulness of data processing performed by controllers and prepare Romania join the Schengen space.

Thus, the number of checks performed to ensure the observance and correct enforcement of personal data processing principles was increased, so 308 investigations and 2 prior checks were performed during 2008 .

Pursuant to the investigations performed, administrative sanctions were imposed consisting of warnings (70) and fines (78). The total amount of the fines imposed in 2008 was of 84,000 lei (RON).

The investigations mainly focused on the activity developed by private data controllers, especially the ones involved in financial and banking activities, e-commerce and the ones that use video surveillance means.

The data controllers that infringed the data protection principles or the rights of individuals were forced to cease personal data processing or the processing of certain data and to erase the illegally processed personal data. There was a case in which the data controller was imposed a temporary ban on processing and a temporary suspension of personal data processing.

Part of the activities developed to prepare Romania's accession to the Schengen space, in 2008, the territorial police inspectorates, the border police inspectorates and other divisions subordinated to the Ministry of Interior and Administrative Reform were investigated to check the conditions governing data processing and the observance of the rights of the individuals as stipulated in Law no. 677/2001 and Schengen acquis .

Special attention was paid to the activities dedicated to the European Data Protection Day, celebrated on January 28th, 2008. The massive participation in the debates held and the interest mass-media paid to this event entitled us to conclude that all the activities organized to this extent reached their aim.

The intensified collaboration with the universities materialized in the active participation of our institution in the international conferences on the topic of personal data protection organized by public and private local universities .

The innovation of this year is that the National Supervisory Authority extended its competencies by virtue of Law no. 298/2008 on the data generated or processed by the suppliers of electronic communication services meant for public use or by public communication networks adopted to enforce Directive 2006/24 EC .

In the context of expanding its competencies, the National Supervisory Authority confronts a real problem, that of insufficient personnel and lack of territorial bureaus able to provide rapid intervention in case of claims and notifications lodged by natural persons.

Our institution has had the same number of employees since 2006 though it was assigned new competencies and new exigencies appeared within the context of Romania's accession to the Schengen space.

We express hope the current document would be a moment of reflection on the existing difficulties to guarantee the right to privacy and on the dangers that may affect private relations .

Georgeta Basarabescu,

President

CONTENTS

CHAPTER I
OVERVIEW

The regulation on the right for private life and on an adequate data protection system is based on the need of each person to decide upon which personal data he may disclose - a value which is safeguarded in a free society.

Starting with the Universal Declaration of Human Rights in 1948 (art. 12) and the European Convention on Human Rights in 1950 (art.8) and the International Pact on Civil and Political Rights in 1966 (art. 17), the right for private life became a fundamental right in important international, regional and European documents.

At European level, the recognition of the right for private life was regulated by the European Council[1] and European Commission[2], as an expression of the preoccupation to create a joint position in the increasing effort to protect private life.

As a result, the local regulations on data protection within European countries have evolved in a dynamic legal framework with stress laid upon the protection of private life and personal data, considered major components of natural person's protection.

In Romania, the Constitution guarantees the right for private, personal and family life. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data represents the National framework law transposing the communitarian regulation on personal data protection - Directive 95/46/EC.

The aforementioned Directive and Law no.102/2005 regarding the setting up, organization and functioning of the National Supervisory Authority for Personal Data Processing (hereinafter referred to as *Supervisory Authority*) bestow upon the Supervisory Authority complete independence, control, consultation, regulating and public information powers in compliance with the communitarian documents .

On national level, the Supervisory Authority has steadily pursue the correlation between its practice with the practice of the other independent supervisory and control authorities, based on the debate of some major problems of the actual world with impact on the right for private life.

During 2008, the activity of the Supervisory Authority, established as part of the average-term strategy, focused on two main courses of action:

- perform investigations in order to ensure the correct implementation of the legislation regarding data protection

[1] Convention no.108 regarding data subject protection, adopted in Strasbourg on January the 28th, 1981.
[2] Directive 95/46/EC of the European Parliament and of the Council on the protection of the individuals with regard to the processing of personal data on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector

- adopt measures to prepare the accession to Schengen space.

Thus, in the fervid Romanian business environment that accompanies the expansion of the economical relations within the European Community and at international level, the Supervisory Authority concentrated the control activities in the private sector that processes a great amount of personal data.

During 2007, the theme investigations aimed at services such as: selection and placement of the workforce, tourism agencies, debt recovery, whilst in 2008, they aimed at the data processed by controllers developing financial, banking and e-commerce activities and using video surveillance systems.

Considering the Schengen assessment visit taking place in the first quarter of 2009, a general action plan for 2008-2009 was drawn, based on two main components: information of the individuals in question and the investigation of the controllers in the public sector, with competencies in police cooperation and granting of visas.

The experience gained as Supervisory Authority in a member state of the European Union and the necessity to strengthen the institutional capacity in view of joining the Schengen space made the Supervisory Authority to pronounce in favour of a legislative proposal for the amendment and supplement of Law no. 102/2005, initiated during 2008. The legislative proposal aimed at consolidating the status of the Supervisory Authority personnel, at increasing the number of personnel according to present and future requirements and at setting up territorial bureaus.

Strengthening the administrative capacity of the Supervisory Authority is needed as by Law no. 298/2008 on the retention of data generated or processed by the providers of publicly available electronic communication services or public communication networks which also amends Law no. 506/2004 on the processing of personal data and privacy protection in the electronic communication sector, the control competencies of the Supervisory Authority expanded.

Pertaining to the highly qualified existing personnel that strove to ensure proper conditions for the activities developed in the context of a significant increase of the amount of works during 2008, the Supervisory Authority continued to train the personnel with the help of Lucian Blaga University in Sibiu, Constantin Brancusi University in Targu Jiu and Hyperion University in Bucharest and with the support of the authorities in the other European countries.

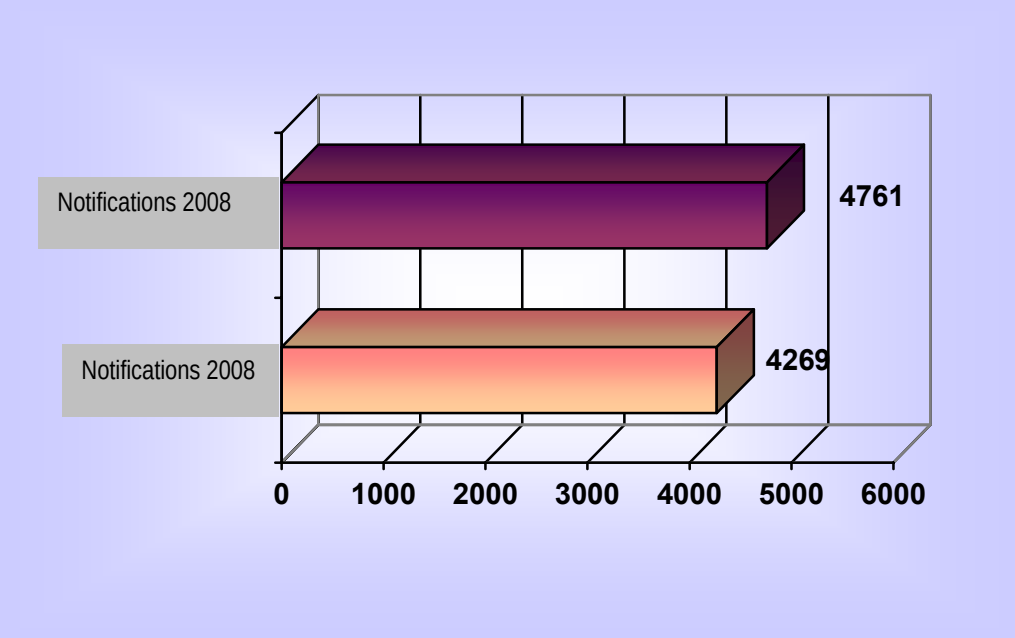
CHAPTER II

SUPERVISION

Part 1: Data processing registration

1.1. The registration of notifications

During the period comprised between the 1st of January 2008 and the 31st of December 2008, the Supervisory Authority received a number of 4761 notifications.



As in previous year, in 2008, the notifications were sent online, by post or they were submitted on paper format to the Authority headquarters.

Starting October 2008, the controllers were encouraged to use the online notifications, beneficial both for the controller, no matter the location in the country, and for the Supervisory Authority. Moreover, the proof that the notification was submitted is obtained very quickly, thus the time needed to send the notification by post is greatly reduced. Likewise, at present, the *online register* on the processing notified by the controllers can be consulted on the site of the Supervisory Authority.

Pursuant to the notifications submitted in 2008, the number of controllers representing judicial executor offices, mutual funds and county recruitment agencies has increased.

Likewise, the number of controllers that use video surveillance techniques (county police inspectorates, border police, educational institutions, controllers in the field of financial and banking services, economic agents) has increased as well.

Thus, a significant number of police controllers notified the processing of offence data on traffic monitoring by empowered persons.

Related to this aspect, the Supervisory Authority considered that the county police inspectorates should set up guarantees for the observance of the rights of the data subjects, in order to avoid an excessive processing of personal data.

Unlike previous years, controllers correctly identified the *scope of the processing, the categories of data subjects, the categories of processed data and of addressees* thus, the Supervisory Authority is entitled to conclude that its short-term and average-term objectives entered the public conscience.

One can easily notice the change in attitude of the controllers in point of observing the legislation relating to personal data protection, of an increased interest in notifying personal data processing, of a correct understanding of the notification form content, of the awareness relating to the necessity to inform the data subjects on the rights they have according to art. 12 - 18 in Law 677/2001 and of the observance of the 'person's consent' principle as a guarantee that the personal data processing is legitimate.

On the other hand, there is still confusion about the meaning of the terms, controller' - 'representative' - 'processor', as they are defined in art.3 letters e) and f) in Law 677/2001 and as a result, some parts of the notification form are not correctly filled in. This confusion appeared especially in case of the entities that activate in the field of credit systems, insurance and re-insurance.

Likewise, there were deficiencies in filling in the notification form as some controllers do not know the instances for which, according to the law, it is possible to fill in the simplified notification form.

Some shortcomings were noticed in relation with inappropriate correlation between the purpose of the processing performed and the period of time established to keep the data stored, longer than the period needed to achieve the purposes of its collection.

By analyzing the data sent by collectors on the occasion of an advertising lottery with prizes, one could notice that the person taking part in the competition has to accept that his name, address and image become public, although as according to Government Ordinance no. 99/2000 regarding

the commercialization of products and market services, the organizer of an advertising lottery is obliged to make public only the name of the winners and the prizes granted.

Likewise, by taking part in advertising lotteries, the person has to disclose personal data, excessive in relation with the purpose of the processing (e.g. personal identification number, series and number of the identity card, marital status, the children and their dates of birth, the spouse's profession).

In relation with the aforementioned instances, the Supervisory Authority requested all collectors to observe the provisions of art. 4 paragraph (1) letter c) in Law 677/2001, of Decision no. 187 of April the 3rd, 2006 regarding the Regulatory Code for Audiovisual Content and of Government Ordinance no. 99/2000.

In response to the requirements of the Supervisory Authority regarding the principles stipulated by art.4 in Law no. 677/2001, and especially the purpose proportion, most of the collectors in question reduced the number of the data processed and they considered only the data necessary to achieve the purpose.

Considering the aspects noticed in relation with the registration of the notifications, the importance of standardization and simplification of the notification procedures of the Supervisory Authority and the necessity to adopt less expensive methods to put them into practice, in order to avoid excessive administrative formalities, the Supervisory Authority issued Decision no. 95/2008 regarding the establishment of a form for the notifications stipulated in Law no. 677/2001 for the protection of persons with regard to personal data processing and free movement of this data.

1.2. Analysis of the annual reports of public authorities

The annual reports of the public authorities regarding the activity in the field of personal data processing shall be submitted to the Supervisory Authority on grounds of art. 21, par. 3, letter j) of Law no. 677/2001. For the year 2008, a significantly increased number of reports was received from these authorities as compared to the previous year.

Part 2: Transfer of personal data abroad

2.1. The regulation of the field

According to the communitarian principles provided in art. 25 and 26 of Directive 95/46/EC, the issue of the transfer of personal data abroad is regulated by art. 29-30 of Law no. 677/2001.

Therefore, art. 29 of Law no. 677/2001 establishes the principle according to which the transfer can be performed only within the conditions in which the state which intends to transfer the data (the destination state) ensures an adequate protection level.

The level of protection of the personal data is considered adequate in the member states of the European Union, namely in the states included in the European economic area: Iceland, Liechtenstein and Norway and in the states for which the European Commission acknowledged, by the Decision, an adequate level of protection. To this extent, by decisions issued based on art. 25 paragraph (6) in the Directive 95/46/CE, the European Commission acknowledged an adequate protection level of personal data for countries such as: Argentine, Canada, Switzerland, Guernsey, The Isle of Man, the United States of America (for the case in which the collector in the USA, recipient of the data transferred from the European Union, acceded the Safe Harbor privacy principles[3]) and Jersey.

The aforementioned decisions of the European Commission were implemented in Romania by the decisions of the president of the Supervisory Authority[4].

Despite of this, considering the fact that data is transferred to states outside the European Union (third states according to the terminology in Directive 95/46/EC) that do not ensure the adequate level of protection for the personal data, the controllers must provide some specific conditions for the observance of the rights of the persons whose data is processed or transferred

In this context, in case the recipient state does not ensure the adequate level of protection, art. 29 paragraph (4) of the law stipulates the possibility for the controller to adopt some contractual

[3] In the USA, Safe Harbor privacy principles and the Frequently Asked Questions issued by the Trade Department of the USA on July 21st, 2000 are applicable; these principles ensure an adequate level of protection for the controllers in the USA, to which personal data is transferred in case these controllers join these principles and fall under the jurisdiction of the Trade Federal Chamber or Transport Department in the USA. The EU admitted that these principles ensure an adequate level of protection for the personal data by the Decision 2000/520/EC.

[4] Decision no.172 /11 December 2006 regarding the adequate level of protection for the personal data in Argentina transposed Decision 2003/490/EC. Decision no. 176 /15 December 2006 regarding the adequate level of protection for the personal data in the Isle of Man transposed Decision 2004/411/EC. Decision no. 173 /12 December 2006 regarding the adequate level of protection for the personal data provided by the Canadian Law on 13 April 2000 transposed Decision 2002/2/EC. Decision no. 174 /13 December 2006 regarding the adequate level of protection for the personal data in Switzerland transposed Decision 2000/518/EC. Decision no. 175 /14 December 2006 regarding the adequate level of protection for the personal data in Guernsey transposed Decision 2003/821/EC. Decision no. 90/2008 transposed Decision no. 2008/393/CE.

measures so that the controller can provide enough guaranties for the protection of the persons' fundamental rights.

The standard contractual clauses represent an important means to ensure the protection of the data transferred from the states of the European Union. By means of the decisions of the European Commission, three categories of model clauses were established that regulate the transfer to controllers or processors in third states. In Romania, these contracts are analyzed in relation with the provisions of Order no. 6/2003 regarding the standard contractual clauses for the transfer of personal data to a controller located in a state for which the law does not stipulate a level of protection at least equal to the one existing in Romania and with the Decision no. 167/2006 of the President of the Supervisory Authority regarding the approval of the standard contractual clauses in case of personal data transfers to a processor located in a state for which the law does not stipulate a level of protection at least equal to the one existing in Romania .

2.2. The notification and authorization of the transfer of personal data abroad

2.2.1. Notification of the transfer

Law no. 677/2001 establishes the rule according to which the transfer of data abroad shall be the object of a preliminary notification of the Supervisory Authority. Due to the risks the data subject may be subject to, there were cases in which, although the data controller is exempted from the obligation to notify processing, he is not exempted from notifying the transfer.

Specific element of data transfer, Law no. 677/2001 stipulates that, in case the controller is not located in Romania, but uses any kind of means on Romanian territory in his activity of data processing, he shall assign a representative, a person located on Romanian territory.

In this context, mention should be made that after Romania become a full member of the European Union, the conditions through which a representative is assigned changed considering the provisions in art. 148 paragraph (2) in the Constitution of Romania and the priority principle of the communitarian right pronounced upon by the European Communities Court of Justice. Therefore, only the collector that is not located within the Community shall assign a representative in Romania.

Another situation is that in which a natural or legal person, of public or private law, processes personal data on behalf of the controller, according to art. 3 letter f) of Law no. 677/2001 and in this case he acts as *processor*. To this extent, Directive 95/46/EC defines the processor as any other body that processes data o behalf of the controller.

Considering the fact that Romania is a full member of the European Union, the constitutional provision in art. 148 and the enforcement of the priority principle of the

communitarian right pronounced upon by the European Community Court of Justice, the processor can be any entity irrespective of his legal status. The processor can be any person that establishes the purpose and the means for personal data processing.

2.2.2. Transfer authorization

Pursuant to Romania's accession to the European Union, the free movement of personal data is guaranteed in the European economic space, and thus it is no longer necessary for the data transfer to the member states of the European Union and within the European Economic Area to be authorized.

To regulate these situations, Decision no. 28/2007 was issued regarding the data transfer to other states. Thus, in case the data transfer is made in the member states of the European Union, in the states in the European economic area, namely Iceland, Liechtenstein and Norway or in the states for which the European Union acknowledged an adequate level of protection, the notification of the Supervisory Authority is needed and not the authorization.

The transfers of personal data to other states than to the ones mentioned previously, performed on grounds of art. 30 of Law no. 677/2001, shall be declared by means of a previous notification, but without being issued an approval from the Supervisory Authority.

Data transfer to a third party is notified and authorized in case it is done based on a contract that includes enough guarantees regarding the protection of the persons' fundamental rights, according to art. 29 paragraph (4) of the Law no. 677/2001.

In 2008, seven transfer authorizations were issued based on standard-clause contracts, out of which two for the personal data transfer to a collector located in a third state and five authorizations for the personal data transfer to a processor located in a third state.

Five of these transfers were made to collectors /processors located in USA that did not accede the Safe Harbor privacy principles.

CHAPTER III

CONTROL

Part 1: Overview

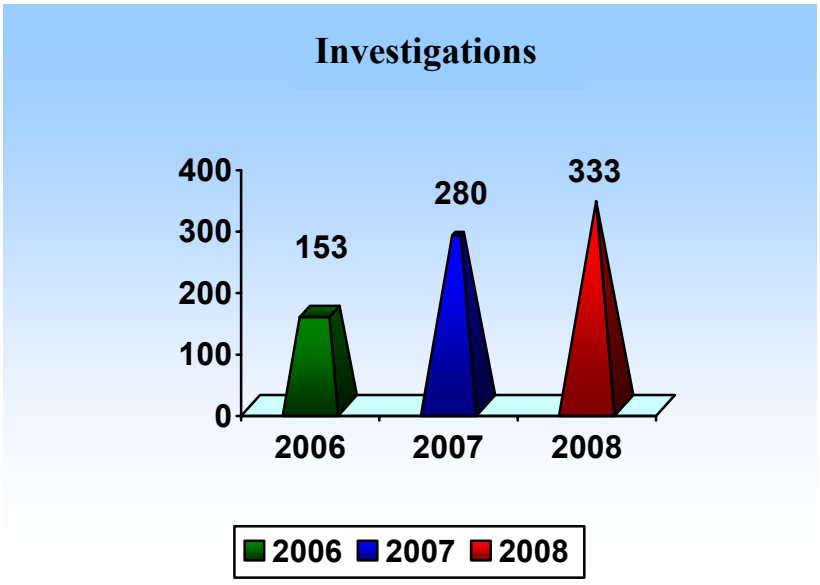
Within the context of personal data processing, one of the objectives established by the strategy of the Supervisory Authority is raising the awareness level of the obligations of the data controllers and of the rights of the data subjects, including by increasing the number of inspections and by applying pecuniary penalties to those who fail to respect the rights of the data subjects

The control activity developed in 2008, though affected by the budgetary restrictions regarding travel expenditures, based both on performing the investigations in the annual planning and on checking possible illegal processing resulted from the complaints and notifications submitted to the Supervisory Authority.

To this extent, mention should be made that the number of complaints greatly increased and a large number of these complaints involved complex issues that needed additional investigations.

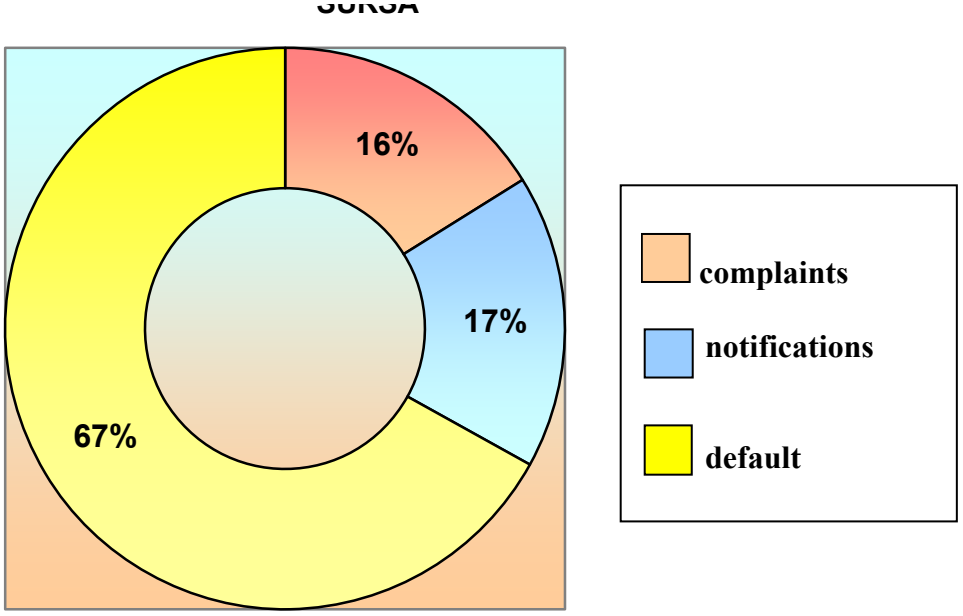
At the same time, most of the complaints received from other public authorities referred to cases in which Law no. 677/2001 was broken as a result of illegal setup and transactions made with personal data bases; for these cases, the Supervisory Authority made all efforts to investigate the aspects indicated.

333 investigations and *2 prior checks* were performed during 2008.



Out of the 333 investigations, a number of 222 were carried out by default, and 111 as a consequence of the submission of complaints (54) and of notifications (57). Out of the 333 investigations, 34 investigations were made in writing.

INVESTIGATIONS ACCORDING TO THE SOURCE



Following the investigations, there were applied contraventional sanctions represented by warnings (73) and fines (78). The total amount of the fines applied in 2008 is of 84,000 lei (RON).

According to the provisions of art. 21 par. (3) letter d) of Law no. 677/2001 and of art. 3 par. (5) of Law no. 102/2005, in the cases in which there was found an infringement of the provisions of Law no. 677/2001, according to the circumstances, there were applied, aside from contraventional sanctions, some specific compulsory measures, by means of the decision of the president of Supervisory Authority. Based on the findings of the investigations, the controllers were addressed 14 decisions, 2 compulsory instructions and 9 recommendations.

Out of the 14 decisions, 12 were issued as a result of the investigations performed and 2 as a result of prior checks.

Therefore, the data controllers who did not obey the principles of the protection of personal data or the rights of the data subjects were forced to cease processing personal data (in 7 cases), and to erase illegally processed personal data (in 10 cases). .

At the same time, in two situations, they ordered a temporary suspension of the activity of data processing.

According to art. 23 of the Law no. 677/2001, amended and supplemented by Decision no. 89/2006 regarding the classification of the categories of data processing operations susceptible of including special risks of the rights and freedoms of the individuals according to the declarations in the notification form sent by the controllers, there were two cases for which prior checks were decided.

The purposes declared in the notifications referred to data processing regarding the state of health in a single medical record organized following the collection of data from the internet and the collection from the internet of the data stipulated in art. 7 of the Law 677/2001, on advertisement, marketing and publicity purposes.

Pursuant to the prior checks, decisions were issued for the controllers to start data processing only after the following conditions are met: inform the data subjects on the rights stipulated in Law no. 677/2001 and submit, fill in /modify the notification according to the recommendations made by the Supervisory Authority representatives in the inspection and sanction report.

In a similar way, there was an instance in which the controller did not correctly interpret the sections in the notification form, thus declaring more data than he initially intended to collect and then process.

The investigations in the field of police cooperation and granting of visas shall be presented in Chapter IV.

Part 2: Theme investigations, according to the annual schedule

Most default investigations pursued the fulfillment of the *annual schedule* drawn up on grounds of certain themes derived from the activity of the Authority, with regards to which it was previously found that Law no.677/2001 was unknown, and there was registered a small number of notifications.

Therefore, the four important themes according to which investigations were carried out throughout 2008 were:

- *SWIFT* – personal data processing performed by financial and banking institutions that use SWIFT services;
- *Medical and health center* – personal data processing performed in the field of health and body fitness services;
- *E-commerce* – personal data processing performed in the field of e-commerce;
- *Video surveillance* – personal data processing , namely image processing, by means of video surveillance.

During the first quarter of 2008, pursuant to the investigations performed in 2007, the theme investigations became necessary, outside the annual schedule, for the following fields:

- *The national program regarding the evaluation of the state of health of the population in primary medical assistance* – personal data processing as part of this program and
- *Diagnosis Related Groups* (*DRG)* – patients' data processing.

Pursuant to the investigations performed, it became clear that the number of notifications received from controllers working in the fields in which the investigations were performed greatly increased.

2.1 SWIFT

As part of the investigations performed according to the annual schedule, the necessity to perform default investigations became clear, as a consequence of the issues approached by the Art. 29 Working Party, namely personal data processing within the SWIFT international financial transactions system.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a cooperative society under Belgian law founded in 1973 that offers its clients in the financial and banking field a secured and standardized messaging system used to facilitate the financial services. As a result, most of the international bank transfers is made with the help of this company, whose services became vital for the parties involved in such transactions.

The use of the services offered by SWIFT program involves the transfer of the personal data from a member state of the European Union (Romania included) to SWIFT operational centers in USA, Belgium or Holland.

As already mentioned in the reports of 2006 and 2007, the European supervisory authorities expressed their opinion on SWIFT issue by means of an Opinion in Art. 29 of the Working Party (the working party has an advisory status, it is established for the European Commission and it is composed of representatives of the supervisory authorities designated by each Member State). Therefore, in the Opinion no. 10/2006, the Working Party underlines the fact that neither SWIFT nor the financial institutions in EU informed the data subjects on the personal data processing and especially on the data transfer to USA and that the limited security measures adopted by SWIFT cannot replace the independent surveillance that may have been provided by the supervisory authorities.

Starting 2006, the Supervisory Authority initiated reunions with the representatives of the Romanian Association of Banks (ARB) and with the representatives of the financial and banking institutions, ARB members, with a view to cease any action that infringe the legal provisions regarding the personal data protection.

At the same time, in 2007, the Supervisory Authority sent the Romanian Association of Banks the necessary elements for an proper information, established according to Opinion no. 10/2006 of the Working Party referred to in Art. 29, the banking institutions that use SWIFT should communicate to their clients.

As a result of the monitor and check activities established by Law no. 677/2001, the Supervisory Authority supervised the way in which the financial institutions observed the obligations they have regarding data transfer in SWIFT transactions to USA and checked, at the beginning of 2008, the information of the data subjects.

From the investigations performed, it became clear that data is transmitted to SWIFT operational centers based on a framework contract concluded by each participant and SWIFT; this contract has the same provisions for all participants, thus the data is processed in a similar way by sending it to SWIFT operational centers.

In order to inform the data subjects on data transfer by SWIFT, the banks use, as methods, the display at subsidiaries' and on their site of the information notes that include data regarding the fact the SWIFT may provide the authorities in USA, on their request, with access to the personal data associated with the transactions made by SWIFT, after September the 11th, 2001. The information note states that the USA Department of Finance may request access to the personal data of the clients of the banks, which is stored in SWIFT operational center with the exclusive purpose

to fight terrorism; this data is stored only for the period of time needed to reach this purpose, in a secure environment.

The checks performed showed that some of the controllers did not notify the data processing they performed to this extent and that some of the financial and banking institutions did not inform as according to art. 12 of the Law 677/2001; corrections were requested.

The controllers follow the recommendations expressed by the Supervisory Authority.

2.2. The national program regarding the evaluation of the state of health of the population in primary medical assistance

The Authority was notified regarding the possible inconformities regarding the way in which personal data is processed within the National Program regarding the evaluation of the state of health of the population in primary medical assistence (hereinafter reffered to as *PROGRAM*), initiated by the Ministry of Public Health.

According to Order no. 994/2007 regarding the approval of methodological norms for performing and for reporting specific activities within the national program for the evaluation of the state of health of the population in primary medical assistance, amended and supplemented, jointly issued by the Minister of Public Health and by the president of the National Health Insurance Authority, the *PROGRAM* started on July the 1st, 2007.

The objectives of the *PROGRAM* are: to assess the state of health of the population and the risk factors in order to maintain and promote health and to prevent illnesses, to know the risk factors for the illnesses that have a major impact on the population state of health, to improve the population state of health by increasing the access to preventive medical assistance and life expectancy, to perform biological and clinical screening in order to discover in time oncologic, cardiovascular, neurological and other diseases based on the risk factors identified pursuant to the assessment of the state of health of the population.

Pursuant to the investigations performed in 2007, whose findings were presented in detail in the activity report of 2007, the Supervisory Authority sent to the Ministry of Public Health the compulsory instructions regarding:

a) completing/modifying the notification with the information resulting from the enforcement of Order no. 994/2007, regarding: the processors, the categories of personal data, the estimated date for the finalization of the processing operations, the futher destination of the processed data, the description of the security measures for data processing;

b) to inform general practitioners involved in the program and the citizens regarding the recipients of the data and regarding the fact that the refusal of the citizens to provide the required

information through the individual risk chart, approved by Order number 994/ 2007, amended and completed, does not draw any consequences;

c) to establish concrete methods of exerting access, intervention and oposition rights by the data subjects in the relation with the Ministry of Public Health and the Health Insurance Authorities;

d) to respect the minimum security requirements for personal data processing, provided by Order number 52/2002, regarding the approval of the minimum security requirements for personal data processing, which establishes the assignment of identification codes, accompanied by logging in methods, by eliminating the possibility for the software application put at the disposal of the Ministry of Public Health to be accessed on basis of the personal identification number of the family medicine doctor.

At the same time, in view of enforcing these compulsory instructions, we recommended the Ministry of Public Health to modify some of the provisions in Order no. 994/2007.

The Supervisory Authority monitored, during the year 2008, the way in which the Ministry of Public Health followed the addressed instructions and recommendations, in a view of respecting the provisions of Law no. 677/2001. Therefore, in February 2008, a meeting was organized with all the important factors involved in the *PROGRAM,* namely representatives of the Ministry of Public Health and of the Health Insurance Authorities, in order to clarify some aspects about the processor assigned by the National Health Insurance Authority within the *PROGRAM,* about the role this processor has in processing personal data and in ensuring the information right for the data subjects and about the necessity to process updated personal data.

The investigations carried out revealed a series of deficiencies from the point of view of the enforcement of Law no. 677/2001.

The investigations in 2008 took place at entities involved in the development of the *PROGRAM*: county public health insurance authorities (hereinafter referred to as *CASJ*), county public health authorities (hereinafter referred to as *ANPJ*), medical services suppliers.

According to Order no. 994 of July 2007 and to the Regulations of June the 4th, 2007 for the achievement and reporting of the specific activities within the national program regarding the evaluation of the state of health of the population in primary medical assistance, the *health insurance authorities* were responsible even for the elaboration, implementation and program monitor.

To this extent, the health insurance authorities conclude contracts with the suppliers in the primary medical assistance and with the suppliers of para clinical services and check, after they receive the documents from the family medicine doctors and from the paraclinical services, the correlation between the personal identification codes included in the summary sheets with the

personal identification codes included in the secured coupons submitted by the medical services suppliers, namely the correlation between the paracalinical examinations recommended by the family medicine doctor.

The family medicine doctors and the para clinical services periodically submit many types of summary sheets to the health insurance authorities. The summary sheets are submitted together with a copy of the patient's coupon. The coupons contain a barcode scanned to validate the coupons, and thus the correlation between the personal identification number and the presence of the data regarding the person in question in the database is checked. Summary sheets can be submitted on floppy-disks, on paper format, as they must be signed and stamped by the family medicine doctor, namely by the representative of the para clinical services supplier.

The investigations prove the fact that, during more sessions, the health insurance authorities managed to train family doctors regarding the *PROGRAM* and the responsibilities they have.

Pursuant to the investigations performed at the county public health authorities', it became clear that the National Agency for Programs within the Ministry of Public Health established the content of the risk charts and developed the software used to collect the patients' personal data as part of the *PROGRAM*. Likewise, it became clear that the county public health authorities do not receive personal data from medical services suppliers. They receive instead from the county health insurance authorities, on a monthly basis, a statistical report that contains the number of the persons evaluated as part of the program, the number of persons with disease risk and the number of paraclinical examinations recommended by doctors, etc. Pursuant to the investigations, it became clear that the county public health authorities submit on a monthly basis to the Prefect's Office and to the National Agency for Programs in the Ministry of Public Health a statistical report regarding the development of the program in the territory .

At the same time, the investigations showed that the county public health authorities involved, together with the representatives of the county health insurance authorities, in training the doctors for the implementation of the program and for the responsibilities they have and in making the *PROGRAM* known.

After the investigations developed at the medical services suppliers', it became clear that the suppliers concluded contracts with the health insurance authorities as part of the *PROGRAM* development. To put this into practice, the patients go to the family medicine doctors with the coupon received, and the doctors fill in the individual risk chart and recommend the medical examinations needed. The doctors do not fill in all the sections of the individual risk chart because this thing depends on the patient and his desire to answer the questions. The individual risk charts were downloaded from the sites of the health insurance authorities.

The investigation performed at the medical services suppliers' showed that the minimal safety requirements are observed when it comes to the patient's data being processed.

The individual risk charts are introduced in the application and transmitted on electronic format to the health insurance authorities together with the summary sheets and the coupons.

The patient's data is transmitted only to the health insurance authorities.

The checks performed in case of the participants in the PROGRAM showed that the information of the data subjects is made, for all cases, in the context of the rights of the patients.

The investigation performed at the National School for Public Health and for Sanitary Management, in the quality of processor, revealed the fact that the school in question did not receive any instructions from the controller - the Ministry of Public Health (MSP) regarding the processing of the personal data included in the lists submitted (name, first name and the personal identification number for the doctors that concluded contracts with the County Health Insurance Authorities and the Health Insurance Authority in Bucharest).

As a result of the analysis of the application used in this *PROGRAM*, the National School for Public Health and for Sanitary Management was addressed a series of recommendations for the improvement of the security measures for the data processing and the Ministry of Public Health was recommended to issue an instruction regarding the personal data processing by the National School for Public Health and for Sanitary Management .

A positive aspect that must be underlined is the fact that the Ministry of Public Health issued Order no. 1392 of August the 4th, 2008 regarding the modification and the completion of the Methodological norms for the accomplishment and reporting of the activities included in the National program regarding the evaluation of the state of health of the population in primary medical assistance, approved by the Order no. 994/354/2007[1] of the Ministry of Public Health and of the President of the National Health Insurance Authority

The provisions in this Order prove the fact that the recommendations and instructions addressed by the Supervisory Authority were acknowledged.

2.3. Diagnosis related groups (DRG)

Diagnosis related groups (DRG) is a system to classify hospital cases depending on the diagnosis. By this system, the characteristics of each patient that leaves the hospital are considered (age, sex, discharge status, main and secondary diagnoses, procedures, weight at birth - in case of newly born and thus patients are classified in a certain category - a diagnosis group). The National School for Public Health and for Sanitary Management created in 2001 an application to be used especially in diagnosis related groups.

DRG involves some stages: data registration, data collection and transmission and data confidentiality - the patients database should be properly managed to prevent unauthorized use of the confidential data regarding the patients that left the hospital.

According to Order no. 1782 of December 28th, 2006 of the Minister of Health regarding the registration and reporting of the hospitalized patients or of the patients on day hospitals, 'hospitals must collect in electronic format a part of the information included in FOCG - General medical report (…)" (art. 7).

The clinical data collected in electronic format from FOCG represents ,the minimal data for each hospitalized patient' (SMDPC). According to art. 9 of the Order, 'hospitals must transmit SMDPC (...) to the National School for Public Health and for Sanitary Management, and to the County Health Insurance Authorities and the Health Insurance Authority in Bucharest (…)".

According to the same Order, the transmission of data is made by e-mail or other electronic means to the addresses mentioned by the National School for Public Health and for Sanitary Management, and by the County Health Insurance Authorities and the Health Insurance Authority in Bucharest. SMDPC must be sent monthly by the 5th of each month.

At the same time, the Order states that 'the training and the support for the hospitals regarding the collection and transmission of SMDPC (...) will be done by the County Health Insurance Authorities and the Health Insurance Authority in Bucharest and similar structures in the ministries and central institutions with own sanitary network, that organize and are liable for the development of this process in every county, under the technical and methodological coordination of the National School for Public Health and for Sanitary Management'.

The checks performed in 2008 showed that both the data of the insured patients and the data of the patients that have no insurance are introduced in an application provided free of charge by the National School for Public Health and for Sanitary Management. The personal data of the patients, collected in the general medical report when the patient is hospitalized, is introduced in the application. .

The data introduced by the hospital employees in the application is sent by e-mail to SNSPMS. When the data reaches SNSPMS, it is classified according to the diagnosis and it is sent back to the hospital under the form of a statistic report indicating the sums that will be allocated to the hospital depending on each patient and his diagnosis.

Patients are informed about the rights they have by displaying this kind of information in hospital wards or waiting rooms.

At the same time, pursuant to the checks performed in hospitals, it became clear that the minimal security measures stipulated in Order no. 52/2002 are observed.

2.4. Health maintenance centers

One of the themes introduced in the investigation plan of 2008 was the control of the observance of the provisions in Law no. 677/2001 and of the minimal security measures regarding personal data processing by the companies that provide health maintenance services as this activity involves, in some of the cases, processing of health data.

According to art. 7 in Law no.. 677/2001, personal health data processing can be performed only with the consent of the data subject.

The investigations performed showed that no all the companies checked has the quality of controllers as defined by art. 3 letter d) of Law no. 677/2001.

The persons that apply for the services offered in health maintenance centers fill in a questionnaire and /or conclude a service contract; personal data is collected by this documents.

There are cases in which a medical record is filled in by a doctor. This record generally includes: anthropometric data, physiological antecedents, pathology, physical deficiencies, cardio-vascular system, etc. The data on physiological antecedents, pathology, physical deficiencies, cardio-vascular system is provided by the patient, at his own risk, without the state of health being practically assessed. This data is important for the collector as it helps the latter to evaluate the impact of some exercises and treatments on the state of health, to evaluate whether some of the exercises are recommended, etc.

The checks performed during the investigations showed that no all controllers notified the personal data processing performed, before the processing start up.

Example:

Company X was sanctioned because it omitted to notify the data processing it performs in order to supply goods and services, before it started the processing in question and because it illegally processed personal data as it did not inform the data subjects about the rights they have according to the law.

By inspection and sanction report, the company received the recommendation to notify the data processing it performs, to inform the data subjects about the rights they have as according to law and to conclude confidentiality clauses with the employees that have access to personal data.

As the company processed the personal identification number and the bank account of the clients, a decision was issued for the company to cease the processing of such data, namely the personal identification number and the bank account, as this was considered excessive as compared to the purpose of the processing - ‚goods and services supply' and ‚advertisement, marketing and publicity' - and to erase all data processed before the decision was issued.

Further checks showed that the controller observed the measures in the report, ceased to process the personal identification number and the bank account, for the purpose of ‚goods and services supply' and ‚advertisement, marketing and publicity', and erased all data processed before the decision was issued.

As a result of the investigations performed at health maintenance centers', the number of notifications submitted by these controllers greatly increased.

2.5. *Investigations in the field of e-commerce*

E-commerce has greatly developed in recent years. Considering the fact that this activity involves personal data processing, including sensitive data (personal identification number, series and number of the identity card), and knowing the risks online collection involves, the Supervisory Authority investigated companies that activate in the field of e-commerce.

The investigations performed showed that any client that wants to purchase products from the sites of the companies that activate in the field of e-commerce can do this by simply creating an account based on username and password. Thus, the clients have the possibility to order the products they want either online or by phone.

Personal data is collected for these clients, no matter the way in which they buy the products: name, first name, address, phone, personal identification number, series and number of the identity card, e-mail, by filling in the online form. According to the declarations of the investigated companies, the personal identification number collected is necessary to issue the invoices.

In the sections ‚Terms and conditions' and ‚Confidentiality policy' displayed on the sites of the collectors, clients are informed about the purpose of the collection and storage of their personal data and about the fact that this data is not to be disclosed. The two sections do not include any information about the rights the clients have according to Law no. 677/2001.

The checks showed that most of the collectors did not notify the data processing performed before the checks. After the checks, the collectors observed this obligation.

Example:

The investigation performed at a company that has activated in the field of e-commerce since 2006 showed that, by its dedicated site, the collector gathers personal data from the persons interested in the products of the company and processes the personal data of the clients, natural persons, that order online products, by keeping a record both in electronic format and on paper that enters the scope of Law no. 677/2001. Through the online form, data such as: name, first name, personal identification number, delivery address, e-mail, phone is requested. According to the

declarations of the company representatives, the personal identification number is needed to issue the invoices, but no other explanations were provided on this topic.

There is an information note in the section ‚Terms and conditions' on the site of the company that includes the categories of personal data of the clients, natural persons, but no references to Law no. 677/2001 or to the rights the data subjects have according to art.12 paragraph (1) of the Law 677/2001.

Considering the findings of the investigation, the collector was sanctioned for having omitted to notify the data processing and for the illegal data processing as the data subjects were not informed as necessary.

Pursuant to the investigation, the order form on the site of the company was changed and the personal identification number was no longer requested.

Based on the findings of the investigation performed, the Supervisory Authority decided that all personal identification numbers existing in the database of the company should be erased as the collector did not present any determined, precise and legitimate purpose for processing the personal identification number according to art. 4 and art. 8 in Law no 677/2001.

The recommendation was put into practice by the collector.

The investigations performed in the field of e-commerce showed that some of the collectors process the personal identification number of their clients, natural persons, by phone or /and online by invoking the provisions of the Fiscal Code and the requirements of the National Agency for Fiscal Administration that request the collection of the personal identification number to issue the invoices, starting January the 1st, 2007. On the other hand, there are collectors that do not collect the personal identification numbers as they say that there are no regulations to this extent.

Considering the provisions of the Law no. 677/2001 and considering the fact that no clauses were identified in the Fiscal Code that state the obligation to collect the personal identification number for the beneficiaries of some products and services in relation with the invoices issued, the Supervisory Authority requested the opinion of the Ministry of Economy and Finance on the existence of some legal provisions regarding the necessity to collect the personal identification number in order to issue the invoices, by observing the legislation regarding the personal data protection.

2.6. Investigations in the field of video surveillance

The video surveillance systems are often used in the contemporary society both in public and private areas in order to prevent any acts that may affect natural persons, goods, public and private properties.

There are many public and private entities that started to use video surveillance systems, mainly to check the movement of persons and goods, the access to certain areas and the access to certain events or situations..

Considering the risks involved by using the video surveillance systems, each state should monitor the data collected and stored by using video surveillance means so that minimal guarantees for the protection of the citizens individual rights exist.

Data processing through video surveillance means has permanently been in the attention of the Supervisory Authority.

In 2008, the Supervisory Authority received a great number of notifications regarding the check of the way in which the public and private entities that use video surveillance means observe the notification obligation .

As a result, checks regarding the data processing by video surveillance were carried out by default or in response to complaints and notifications received from data subjects.

To perform these investigations, the following were considered: to make the controllers observe the minimal security measures, to express a clear and legitimate purpose, the prevent the data collected by video surveillance systems from being excessively stored, to offer the data subject the possibility to exercise the rights he has according to the law and to avoid disclosing the data processed by these systems without any legal ground.

The purpose invoked for the use of the video surveillance system was the prevention of thefts and other illegal deeds. The images collected are stored on servers for a period of time, depending on the disk capacity, and then they are automatically erased. In case of offences, the images are disclosed only to the police based on an official note.

Example:

The collector investigated as a result of a notification received processed personal data , namely images, by using video surveillance cameras in a restaurant.

The findings showed that the cameras were installed in the toilets too and they allow identification of the persons caught on tape. The purpose declared by the collector was ‚the security of the building and of the goods and the prevention of offences'.

The warning note that the restaurant had video surveillance systems installed was placed only at the entrance of the restaurant.

As the collector did not notify the personal data processing he was sanctioned for the omission to notify and for dishonesty.

Pursuant to the investigation performed, considering that the toilets are exclusively meant for the persons that are using them, the Supervisory Authority considered as excessive the video surveillance cameras mounted in the toilets. The same was the opinion of the Working Party expressed in art. 29 of the Working document no. 67/2002 regarding the personal data processing by video surveillance means.

Considering the above mentioned, the Supervisory Authority decided that the controller should cease processing the images of the persons that use the toilets in the restaurant and erase all data previously collected.

In the case of the video surveillance systems installed to fulfill the obligations in Law no. 4/2008 regarding the prevention and fighting the violence during competitions and sporting games, the Supervisory Authority investigated important football clubs in the country and in Bucharest, where the findings showed that, in most of the cases, the data processing (images) were not notified before the processing was initiated, so the clubs in question were sanctioned.

On the other hand, in most of the cases, the controllers informed the data subjects about the video surveillance systems operating on the football fields both by notes displayed visibly and by oral warnings launched during the competitions.

2.7. Investigations in the field of databases and electronic communications

The Supervisory Authority respects and protects privacy and private life including electronic communications according to Law no. 506/2004 and to Law no. 365/2002. At the end of 2008, the Supervisory Authority received additional duties in this field by adopting Law no. 298/2008.

Regarding the enforcement of Law no. 506/2004, the control activity of the Supervisory Authority developed in two sectors for which the provisions of this law are enforceable: receive unsolicited commercial communications and supply information services about the subscribers.

For the first sector, the investigations were developed as a result of the complaints submitted to the Supervisory Authority; these complaints will be considered in a further section of the current report.

Another aspect worth mentioning is the attention paid by the Supervisory Authority to the complaints regarding the offers received for databases transaction. By this kind of transaction, databases consisting of hundreds of thousands of e-mail addresses and phone numbers can be

devised and the commercial communications continue to be made by using electronic communication services to recipients that did not express their consent to this extent so by breaking the Law no. 506/2004.

As for the second sector regarding information supply services, the Supervisory Authority involved in eliminating from the public sources, like Internet, the illegal databases that include personal data (phone numbers) of some subscribers that were not informed about the existence of these databases.

Examples:

a. Starting from the general aspects mentioned in a complaint, the Supervisory Authority noticed on an internet page counter search services for the phone numbers of the subscribers of different phone companies. Thus, depending on the phone number introduced in the subscribers registry, the service displayed the personal data of the person in question (name, first name, address), without the consent of the subscriber.

For the respective site, during the investigation performed at the company that registered the site in question, the legal representative declared that the site does not belong to the company he manages but to a natural person in USA, whose identity he does not know, and that the server for this service is located in USA. The controller admitted that he only hosts the domain and that he has no access to the subscribers database, that he does not know the source and the destination for the personal data of the natural persons included in this database.

The company in question was authorized at the former National Regulatory Authority for Communications and Information Technology as electronic communications services supplier and networks supplier.

The subsequent checks performed by the Supervisory Authority showed that neither of the two phone companies whose subscribers appeared in the database accessible through internet allowed the subscriber registries to be used to purposes other than a simple search after name and after a limited number of parameters and that their databases were not transferred, free of charge, to other natural or legal persons in Romania or from abroad. Likewise, the findings showed that none of the subscribers was informed about the use of his personal data by the controller and could decide which of the personal data to be sent to that respective site. Both companies notified the company that registered the domain in question and the company that hosted the aforementioned domain to cease the illegal actions.

In relation with the findings of the investigations and with the communitarian and national legal provisions, the Supervisory Authority decided that the controller should meet the following conditions:

- to obtain the consent of all subscribers so that their personal data could be included in the subscribers registry published online and could be used to a different purpose than the one of simply searching the contact data, based on the name and on a limited number of parameters;

- to inform the subscribers about the purpose of such a registry in which personal data can be included, and about any other possibilities to use their data, based on search functions integrated in the electronic registries;

- to explain the way in which the subscribers were offered the possibility to decide upon which personal data will be included in a public registry.

In case the controller does not observe the obligations he has in due time, then he must cease processing the subscribers data and erase this data no matter the storage format.

Pursuant to the investigation, the site in question was suspended.

b. A ministry notified the Supervisory Authority about the existence of some public access servers that contained databases including information about natural and legal persons in Bucharest.

The findings of the investigations showed that one of the databases from the servers, 'Phone directory 2004', allows the search of the natural persons by name, first name, address, locality and displays the phone number. The database and the respective application were created by a natural person and additional information about this application could be found on his own site that included an updated version of the application 'Phone registry and companies 2008'. A demo version of the application could be downloaded and then the application could be purchased by potential clients.

The findings of the investigation showed that the application contained more than 3,000,000 phone numbers collected by the investigated natural person by using a free application available on the internet at a certain moment. The application included the name, first name, street and number, or only the street name, county, locality and the phone number and allowed the search by name or first name of the natural person or by the person's phone number.

Both the application used as data collection source and the database were deleted from the internet as a result of the intervention of the Romanian Police General Inspectorate in 2005.

As a result, the data collection source mentioned above was illegal and it broke the provisions of Law 677/2001.

Moreover, the phone company whose subscribers appeared in the database notified the Supervisory Authority that it did not authorized the use of the databases by the owner of the internet domain.

Pursuant to the findings, the natural person was sanctioned for having omitted to notify and for illegal notification, under the form of omitted notification, of the Supervisory Authority

regarding the data processed on that site. At the same time, the controller-natural person was sanctioned because he could not prove the fact that he obtained the personal data with the clearly expressed consent of the data subjects or from authorized public sources in the case of personal data that exists in the 'Phone directory' application.

At the same time, the Supervisory Authority decided that the controller must cease to process the personal data included in the ‚Phone directory' and erase the data processed before the decision was communicated.

As a result of the investigation, the site became inactive.

2.8. Investigations regarding data disclosure by election lists

After the local elections of June 2008, more citizens notified the Supervisory Authority about irregularities regarding personal data processing by displaying the election lists outside the polling stations during the elections of June the 1st and June the 15th, 2008. The copies of the election lists included the following personal data: personal identification number, series and number of the identity card.

According to Law no. 35/2008 on the election of the Chamber of Deputies and of the Senate and the amendment and completion of Law no. 67/2004 on the election of local public administration officials and the Law of public administration no. 215/2001 and the Law no. 393/2004 regarding the statute of local elected officials, *‚the permanent election lists shall include, in order of the number of the voters' apartments, the name and first name, the voters' address, the personal identification number and the number of the vote card ... ...'*. According to the same law, *'election lists are drawn up and made public no later than 45 days before the election day'.*

According to Law no. 35/2008, the polling stations *shall receive from the National Center for the Administration of Databases regarding Personal Records in the Ministry of Interior and Administrative Reform, no later than 24 hours, two copies of the permanent election lists; one of the copies shall be displayed so that it can be seen by voters;* ***the copy displayed in such a way shall not include the personal identification code, the series and number of the identity card'*** .

Law no. 67/2004 on the election of local public administration officials states that *‚the National Center for the Administration of Databases regarding Personal Records in the Ministry of Interior and Administrative Reform provides town halls with three copies of the permanent election lists that include voters in each polling station. The copies of the election lists are submitted by the mayor, in two copies, based on receive protocol, to each president of the polling station, three days before the election day. One copy is offered to the voters to be consulted and one copy is used on election day'.*

In relation with the aforementioned, the Supervisory Authority requested the Permanent Election Authority to express its point of view on the matter. Thus, as the status of the permanent election lists is not clearly defined in case of local elections, namely if these lists can be displayed in a similar way as in case of general elections, without containing the personal identification number and the series and number of the identity card, the decision made was that the provisions of Law no. 35/2008 should be enforced in a similar way for the election of local public administration officials in order to ensure a legal and non-excessive data processing as stipulated in Law no. 677/2001.

The Permanent Election Authority underlines the fact that the lists should be consulted so that each voter can check the permanent election lists only for his own personal data and this is the reason for which the Authority considers that, according to the law, the lists should not be displayed so that the uncontrolled movement and the illegal use of this data is prevented.

At the same time, the Permanent Election Authority admitted that it did not consider the correlation between the provisions in art. 16 paragraph (6) and in art. 18 of the Law no. 67/2004 and the provisions in art. 20 of the Law 35/2008, according to which the copies of the election lists are displayed visibly but without containing the personal identification number and the series and number of the identity card when the regulation meant to improve and optimize the Romanian election legal framework was drawn up.

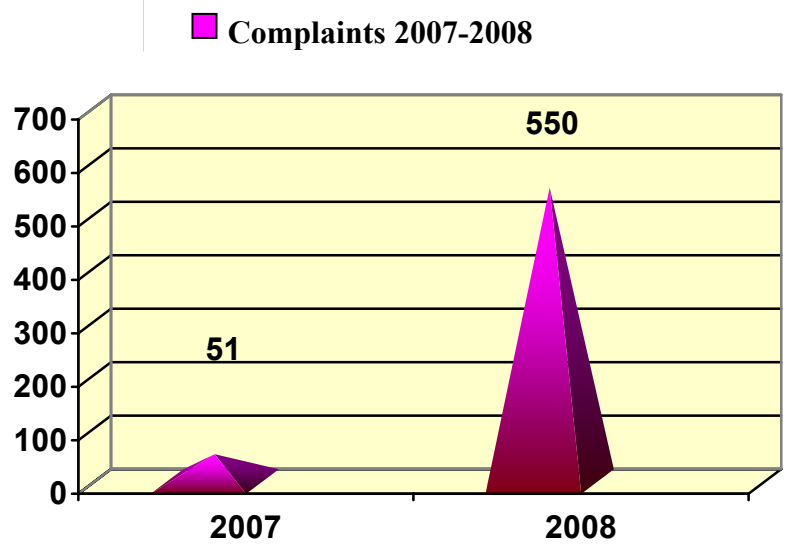
Pursuant to the actions taken, the Supervisory Authority recommended the mayors mentioned in the notifications sent by petitioners to take all necessary measures so that any natural person interested in the list could consult the copies of the election lists on the occasion of the election of local public administration officials and on general elections only for own personal data, so that the data protection for third parties is ensured.

The purpose of these recommendations was to ensure the observance of the fundamental right for private, intimate and family life safeguarded by art. 26 in the Constitution, the observance of the personal data protection and of the principles of the art.4 in Law no. 677/2001, and especially those regarding a legal and non-excessive processing of the personal data for the purpose of consulting the election lists.

Part 3: The activity of solving complaints

Data subjects who consider themselves offended by personal data processing method, may address complaints to the Supervisory Authority, on condition of not having filed for a similar action with the same object in court. The law provides the obligation of the person concerned to previously (15 days before the submission of the complaint) submit a petition to the respective data controller, before submitting it to the Supervisory Authority.

During 2008, the Supervisory Authority received a great number of complaints as compared with the previous year, namely 550 complaints compared to only 51 complaints in 2007; these complaints drew attention on possible infringements of the rights regulated by Law no. 677/2001 and by Law no. 506/2004 and proved that the attributions of the Supervisory Authority became known to the public and that the citizens have more trust in the efficiency of the surveillance activities for this field.



The increased number of complaints submitted to the Supervisory Authority made the monthly investigation plans to be changed so that the investigations performed to solve the complaints should come first.

On the other hand, the deadline of 30 days from the moment a complaint is received stipulated in Law no. 677/2001 necessary to issue a decision of cessation or suspension of illegal processing or to erase the personal data collected and processed without considering the legal obligations proves to be insufficient for a detailed investigation of the complaints submitted to the Supervisory Authority and for collecting the evidence needed to impose one of the coercive measures mentioned above.

As a result, it became necessary to increase the personnel number and to amend the provisions of Law no. 677/2001 regarding the decision to cease or suspend some illegal processing or to erase personal data collected and processed by breaking the legal obligations, within 30 days from the moment a complaint is received.

Most of the complaints had as object the unsolicited commercial messages received, the personal data of the debtors of the different banks which was sent to the Credit Office or to the Banking Risks Central Office and the illegal disclosure and processing of the personal data in other circumstances.

By analyzing the complaints received, one could see that some petitioners do not know the prior legal procedure to submit a complaint to the Supervisory Authority (namely a complaint for the Supervisory Authority cannot be submitted earlier that 15 days from the moment a complaint with a similar content was sent to court) although art.25 of the Law no. 677/2001 states otherwise.

For the well-founded instances (mentioned in detail below), sanctions were enforced and, as the case may be, by the decision of the president of the Supervisory Authority, data processing was ceased, the processed data was erased or the data processing was suspended.

The reasons for rejecting the complaints filed by the data subjects were:

- *not respecting the procedure provided by the law;*
- *complaining against facts which were not of the material or territorial competence of the Supervisory Authority, such as: the refusal to provide documents which contain personal data following the exertion of the free access right to public information, the refusal to provide data regarding third parties; the receipt of commercial communication specific for direct marketing from data controllers who are not located in Romania, by means located on the territory of other states;*
- *not providing proof to support the complaint;*
- *prior action filed in the court.*

3.1. Sending unsolicited commercial messages

During 2008, the number of complaints regarding the unsolicited commercial messages greatly increased, representing almost 60% of the complaints registered at the general registrar of the institution. The messages were sent by e-mail, phone and SMS.

Besides the general competence stated by Law no. 677/2001, the Supervisory Authority was given special responsibilities by Law no. 506/.2004 regarding personal data processing and the protection of privacy in the sector of electronic communications and by Law no. 365/2002 regarding e-commerce.

By the *complaints* addressed to the Authority, the data subject notified the authority of the repeated receipt of unsolicited commercial messages, despite his expressly manifested opposition. .

Each complaint was analyzed and interpreted by considering the provisions in Law no. 677/2001, in Law no. 506/2004 and in Law no. 365/2002. The last law mentioned defines commercial communication as ‚any kind of communication that aims at promoting, directly or indirectly, the products, services, image , name, company or logo of a business person or member of a regulated profession’.

On the other hand, the complaints considered as not entering the commercial messages definition were rejected: 'the following shall not be considered commercial messages: information that enables free access to the activity of a natural or legal person and especially on domain name or on an e-mail address, communications regarding the products, services, image, name or brands of a natural or legal person made by a third person, independent from the person in question and especially for the cases in which these messages are sent free of charge'.

In the context of Law no. 677/2001 and of Law no. 506/2004, for the cases in which the petitioners notified aspects of the type mentioned above, representing commercial communications in the line of Law no. 365/2002 and the prior procedure was followed, the controllers in question were investigated to check the aspects mentioned in the notifications.

In case of acceptable complaints, the Supervisory Authority performed some investigations meant to check if the persons that sent commercial communications to the petitioner had obtained the latter's consent to send this kind of messages to his e-mail address and if they offered him the possibility to reject receiving such messages in the future.

Example:

During one of these investigations, the findings showed that the company whose e-mail address was used to send the commercial message is registered as personal data operator for data processing to the purpose of internet and tourism services. The company processes personal data of the customers /potential customers, such as: name, first name and e-mail address, directly obtained from the data subjects or their legal representatives.

Practically, the persons interested in the offers of the company directly address the company by e-mail or by using the site where some fields should be filled in with personal data, so that the company receives 'the request' from the customers /potential customers. In case one of these customers does no longer want to receive newsletters, he may send an e-mail to the company to request this thing, and this results in his e-mail address being immediately erased from the database. The messages sent observe art. 12 paragraph (2) and (3) of the Law no. 506/2004, even though they erroneously refer to CAN SPAM ACT 2003 - applicable law in USA but not in Romania or European Union.

Regarding the e-mail address where the petitioner received the unsolicited commercial message, the investigated controller admitted that he had sent commercial offers by e-mail, even if on the investigation date, that e-mail address had already beed erased from the electronic registers of the company.

According to Law no. 506/2004, the commercial communication by e-mail is forbidden excepting the cases for which the subscriber agreed on receiving such communications.

As the controller sent commercial communications by e-mail from one of his e-mail addresses, without being able to prove the prior consent of the petitioner, the conclusion was that the controller sent commercial communications by using automated access systems that do not need any human operator, fax or e-mail or any other method that uses e-communication services without the consent of the recipient.

The controller was sanctioned and was forced to change the content of the text that accompanies the commercial messages sent by e-mail, according to Law no. 506/2004 and not to a legislation which is not in force on Romanian territory.

The data controller complied with the recommendations of the Supervisory Authority.

3.2 Credit offices

The *complaints* submitted to the Supervisory Authority regarding possible breaches of the right for family, private and intimate life by personal data processing within credit offices mainly refer to the transmission of the personal data to participants, without observing the provisions in Law no. 677/2001 regarding the rights of the data subjects and without their consent and the provisions of Decision no. 105/2007 of the president of the Supervisory Authority regarding the personal data processed within the credit offices[5].

On February 26th, 2008, Decision no. 105/2007 came into force; the Decision establishes some conditions for reporting the debtors' data by the collectors within credit offices, namely: limited periods of time to store personal data, to ensure the prior information of the debtors, the content of the information, etc.

The Authority also received complaints through which the petitioners, by exercising the rights they have according to Law no. 677/2001, invoked the fact that the controllers, financial and banking institutions, did not reply within the 15 days stipulated by Law no. 677/2001.

Example:

A petitioner signalled a possible infringement of the right to intervene upon data complaining about the fact that, on her request for a credit refunding, she was informed that according to the credit report issued by the Credit Office in 2007 she appears as having a credit of 171 lei at a different bank, although the credit was paid off and there were no overdue payments.

The petitioner addressed the bank that had sent the report to the Credit Office, she obtained the confirmation of the fact that there were no overdue payments and the petitioner's data registered with the Credit Office was to be erased.

[5] Published in the Official Gazette of Romania no. 891 of December the 27th, 2007, Part I.

Despite the above mentioned, the petitioner claimed that by the date of her complaint her application was not solved, according to the data in the last credit report she requested

On the investigation date, by considering the documentation existing at the bank', it became clear that none of the incidents of the kind signalled to the Credit Office existed.

The explanation of the fact that the petitioner continued to appear as having debts with the bank was, according to the bank' representatives, an error in the mechanism that monitors the deadlines and accounts of the bank clients.

The fact that the bank, despite the petitioner's intervention, did not take measures to retrieve the erroneous data and infringed the rights stipulated in art. 14 of the Law 677/2001, represent an offence, so the collector was sanctioned accordingly.

Pursuant to the intervention, the bank erased the petitioner's data from the Credit Office.

3.3. Personal data disclosure

3.3.1. Personal data disclosure on sites

a. By the *complaints* submitted to the Supervisory Authority, many data subjects signalled the use of their data on different sites without their prior and clear consent.

One of the petitioners signalled the fact that his personal data (name, first name, personal identification number and address) was published, without his consent, on the site of some tax office. After having paid the debt and proved to have addressed the collector, the petitioner notified again the Supervisory Authority because his data was still visible on the site mentioned in the notification.

To find a solution for the notification, the respective tax office was checked.

According to the operational regulation valid for tax offices, one of the responsibilities these tax offices have is to draw up and transmit the reports for the natural persons for which tax documents were issued and communicated but the persons in question did not confirm receiving these documents.

The procedure for publishing the debtors' data on the internet is:

The list with taxpayers-debtors comprising personal data (name, first name, personal identification number and fiscal address) drawn up by the tax office is submitted to the county tax office. The personnel uploads the list in electronic format directly on the site of the ministry. The application allows the data to be visible for 30 days; after this period, the data is automatically erased from the site. According to the things declared by the tax office representatives, it is not necessary to fill in all the fields in the application.

The tax office received the recommendation not to disclose the personal identification number of the taxpayers-debtors, in the line of the recommendation made by the Supervisory Authority to the Ministry of Economy and Finance (MEF) since 2007.

To clear up the circumstances that generated the instance notified by the petitioner, an investigation was performed at the Ministry of Economy and Finance.

The fiscal documents may be made publicly according to an order issued by the Ministry of Public Finance that stipulates that the fiscal document may be displayed on the Internet page for a period of 15 days. Moreover, the order stipulates that the data that is to be made public, namely: name, first name, fiscal address, fiscal document, number of date of the document, so without the *personal identification number.*

The investigation performed proved the fact that the lists could be accessed on the internet even after 4 months from the moment they were displayed, by checking the name of one of the persons in the list, with the help of a search engine, due to the storage of the information in the *cache* memory.

Pursuant to the investigation, the Ministry of Economy and Finance was requested to find a solution so that the overdue lists can be no longer accessed, even if the lists continue to exist on the site of the ministry.

The issued was solved by the ministry and the petitioner was informed that his data was erased from the internet.

b. By a written request, a petitioner notified the Supervisory Authority on a possible infringement of his right to private, intimate and family life due to the disclosure of his personal data, without his consent, by a public institution.

In fact, the petitioner complained about the fact that on the site of that public institution, a report of the Discipline Commission was published in which the personal data of the petitioner was mentioned. At the same time, the petitioner claimed that the report in question was the only one of the kind published on that site.

The findings of the investigations showed that:

The collector justified the publication of the report by the petitioner's inappropriate behaviour (who no longer had any professional relation with that public institution on the moment the report was published on the internet) that contravenes the principles that govern the professional behaviour of the public clerks working in the public administration.

By the publication of the report drafted by the Discipline Commission, the disclosure of the personal data was made under different circumstances than the ones stipulated in Law no. 677/2001 that require that personal data processing to be performed in good-will and by observing the legal

provisions in force and in a proper and non-excessive way in relation with the purpose for which this data is processed. The report published may affect the right for defence and the assumption of innocence unless proven guilty which are guaranteed by the Constitution.

Pursuant to the investigation, the Authority decided that all personal data included in the report of the Discipline Commission to be erased from the site and forbade any future personal data processing without observing the provisions of Law no. 677/2001.

In response to the above mentioned, the public institution completely erased the report from that internet page.

3.3.2. Personal data disclosure by debt recovery companies

A petitioner claimed that his personal data was communicated to a third party by a phone company, without being previously informed about this disclosure. But before that, the petitioner claimed the same thing to the collector and he was given no answer by the time of the investigation.

The investigation proved that the collector sent the debtors' data to third parties in order to recover the debts. The data transmitted also included the personal identification number, although the information note sent to the clients regarding the rights stipulated by art. 12-18 of the Law no. 677/2001 clearly specified that the personal identification number will not be included in the data transmitted.

The collector could not prove the fact that he informed the petitioner before the data was transmitted to the debt recovery company and this infringes the provisions in the art. 12 paragraph (1) letter c) of the Law no. 677/2001, namely the information of the data subjects about the data recipients.

Pursuant to the findings of the investigation, the collector was sanctioned for having omitted to notify the Supervisory Authority and for dishonest notification, as the collector did not notify the Supervisory Authority about the processing of the personal identification number and for illegal processing of personal data as the data subjects were not informed about this issue.

As a result of the investigation, the collector informed the third party recovering debts on his behalf that he withdraws all claims against the petitioner and he requested that all data about the petitioner to be erased.

3.3.3. Illegal processing of personal data

a. A petitioner notified the Supervisory Authority that a university transferred her personal data (name, address, personal identification number) to a bank, without her consent, to have a card issued.

The petitioner proved that she first addressed the university and the bank but she was not satisfied by either of the answers, so she finally submitted a complaint to the Supervisory Authority.

To clear up the issue, the Authority investigated both the university and the bank and the findings showed that the university had a contract concluded with the bank based on which cards were issued for the payment of the employees.

An addendum to the above mentioned contract was signed and this stipulates that on each university year start, the bank must receive from the institution a folder with the students, including: name, first name and personal identification number.

The findings showed that the bank did not conclude an individual contract with each of the students for the issuance of the cards and that the cards were taken by the institution representatives based on a receive protocol.

The petitioner was not informed about the issuance of this card and about the transmission of her personal data to the bank. By considering the contract concluded by the petitioner with the university, it became clear that the petitioner did not express her consent for her data processing; the registration form includes only a general consent for personal data processing by the university.

After a period of time, until the moment of the investigation, the university changed the contract format, namely the tuition fee for the next semester can be paid by bank transfer, using the card provided to the student; this information is also available on the university site mentioned in the contract.

The students that wanted to take their cards signed in a table, near their typed name (card number, card account, holder and address). The petitioner did not take her card so her data was erased and the card cancelled.

The findings of the investigation showed that the university illegally processed personal data as it did not obtain the petitioner's consent to transmit the personal identification number to the bank and did not inform the petitioner about the data sent to the bank or about the purpose of this disclosure. As a result, the university was sanctioned.

During the investigation, the bank representatives admitted that there was an error in processing the petitioner's personal data for the purpose of issuing a new card as there was no prior check of the consent and of the information of the petitioner.

According to BNR Regulation no. 6/2006 regarding the issuance and use of the electronic payment tools and the relations between the participants to the transactions performed with the help of these tools, the electronic payment tools shall not be put at the disposal of any natural person provided a prior consent or written request from the person in question exists.

Moreover, the name, first name and personal identification number can be processed only with the prior consent of the data subject unless otherwise stated.

At the same time, the controller is obliged to provide the data subject with some information regarding the identity, the purpose of the processing, the data categories, the data recipients, the rights of the Law no. 677/2001 and the conditions necessary to exercise these rights on the moment he collects the data but no later than the moment of the first disclosure.

The bank could not prove the fact that the legal obligations were observed from the moment it collected the petitioner's data and to the moment the petitioner addressed the bank.

According to the findings of the investigation, the petitioner's data was erased from the bank records at the same time with the closure of the bank account.

For the illegal processing of the personal data as a result of issuing a card without the prior consent and information of the petitioner, the controller was sanctioned.

b. Another natural person notified a possible illegal processing of his personal data by the Construction Discipline Department within a local council, to the extent to which an inspector working in this department, having at his disposal a copy of the petitioner's identity card (the copy was retained to draw up an inspection and sanction report that was cancelled in the court at a later date), used data from this document when he drew up, in the petitioner's absence, a new inspection and sanction report.

Pursuant to the complaint submitted by the petitioner, the Construction Discipline Department within the town hall responded that it has a copy of the identity card, annex to a protocol signed by the petitioner in quality of witness and offered no further details about the way in which his personal data was processed.

The findings of the investigations showed that the town hall, according to the organizational chart approved by a decision issued by the local council, processes personal data through other structures as well, even though these structures are not legal entities.

Pursuant to the investigation, the town hall was sanctioned as it did not notify the personal data processing performed as part of the activity developed in the Construction Discipline Department.

The Supervisory Authority recommended that the employees of the town hall should be trained on the enforcement of the provisions in Law no. 677/2001 and especially on the legal and in good-faith processing of the personal data needed to draw up the reports according to the Government Ordinance no. 2/2001; in this context, the personal data of the witnesses shall not be used when drawing up inspection and sanction reports in the future.

Moreover, the Supervisory Authority recommended that the personal data contained in the inspection and sanction reports should be stored for a limited period of time, that technical and organizational measures should be taken in order to allow the access of the town hall employees to the personal data included in the inspection and sanction reports, that measures should be taken to

notify all data processed by the town hall as part of the activity developed and that the notifications already submitted should be checked to see if they need further completion or /and modification.

Pursuant to this investigation, the town hall followed all instructions and recommendations addressed by the Supervisory Authority.

CHAPTER IV
PREPARATION OF THE ACCESSION TO THE SCHENGEN AREA

Part 1: Joint Supervisory Authority

In order to prepare Romania join the Schengen space, one of the priorities of the Supervisory Authority was the active participation in the Joint Supervisory Authority reunions (JSA), founded according to the provisions in art. 115 of the Convention implementing the Schengen Agreement (CISA) as authority empowered with the supervision of the technical assistance department of the Schengen Information System.

In this context, the Supervisory Authority mainly considered the adjustment of the relevant legal framework to the Schengen acquis and the correlation between its practices with the ones specific for JSA and for other supervisory authorities in the signatory states of the Schengen Agreement.

The Supervisory Authority was involved in the activities developed by the other joint supervisory authorities in the field of police and judicial cooperation - Europol Joint Supervisory Body (JSB), Joint Supervisory Authority - JSA Customs, Eurodac Supervision Coordination Group and Working Party on Police and Justice (WPPJ).

Part 2: The duties of the Supervisory Authority

In January 2008, Romania and Bulgaria signed the joint declaration on the accession to the Schengen space; according to this declaration, Romania and Bulgaria establish 2011 as date of their joint accession to the Schengen space and decide to take common steps to reach this objective. By this document, Romania expresses its intention to start, from the second half of 2008, the assessment process in the fields of personal data protection, police cooperation and visas.

To prepare Romania's accession to the Schengen space, new national regulations must be adopted and the regulations already in force must be changed so that they align with the European legislation in force in the fields assessed. The legal alignment must ensure the protection of the

fundamental rights and freedoms and especially the right for private life. To this extent, the protection of the data subject is very important considering the forecast information flow.

In the field of personal data protection, according to the provisions of the Convention implementing the Schengen Agreement (CISA), the National Supervisory Authority for Personal Data Protection is the control authority that independently supervises the data file in the national section of the Schengen Information System and checks if the data introduced and used does not infringe the rights of the data subject.

In order to reach the objectives related to the preparation of Romania's accession to the Schengen space, during 2008, the Supervisory Authority established a short-term strategy that includes organizational measures, personnel training, information campaign for the data subject, cooperation with the competent authorities to implement the Convention implementing the Schengen Agreement (CISA) and checks performed at the competent authorities (police, border police, consulates, International Police Cooperation Center, Romanian Immigration Office, etc).

Part 3: Organizational measures at the level of the Authority

On grounds of the provisions of the Organizational Regulation valid with the Supervisory Authority, by the decision of the president of this Authority, the persons to activate in the field of data protection were nominated. These persons will supervise the extent to which the Authority fulfills its duties in order to prepare Romania join the Schengen space and will prepare the necessary materials for the assessment.

In this context, the activities meant to inform the data subjects on their rights as they derive from Law no. 677/2001 and CIAS and the investigations developed at the authorities responsible for providing and /or analyzing the complaints contained in the National Schengen Information System will be intensified.

To reach the objectives proposed in the Schengen assessment process, the personnel of the Authority is continuously trained at the level imposed by communitarian standards, disposes of documentation, takes part in work groups and in experience exchanges in member states of the European Union.

Therefore, it is important to mention the participation of the Supervisory Authority representatives at the seminar entitled 'Data protection for police and judicial cooperation in criminal matters: EU requirements', organized with TAIEX help, in collaboration with the Academy of European Law. The objective of this seminar was to offer a detailed image of the international and European legal tools in the field of data protection. To this extent, attention must be paid to the data protection requirements that are to be observed in relation with the information exchange

within the Schengen Information System and with the information exchange with EU bodies for police and judicial cooperation in criminal matters.

Part 4: Information campaign

During 2008, the Supervisory Authority carried out specific activities across the country, in order to increase the people's level of awareness and information regarding personal data protection; these activities were also included in the Convention implementing the Schengen Agreement.

Materials on the rights of the data subjects, also as part of the Convention implementing the Schengen Agreement, were distributed especially at the borders as these areas are considered of great importance in point of personal data processing, part of the Schengen Information System.

An important moment for the activity of the Supervisory Authority and especially for personal data protection is represented by the European Day for Data Protection. In 2008, this event was organized in Targu Jiu, with the help of the Police Inspectorate in the Gorj county, and it proved to be a real success. As part of the event, an exhibition was organized. In the second part of the meeting, attended by the representatives of the county police inspectorates and representatives of the structures subordinated to Gorj Police Inspectorate, aspects on Schengen issue and the importance of data protection in the police sector were discussed.

At the same time, the Supervisory Authority organized seminars and meetings at central and territorial level. In March 2008, the ‚train-the-trainers' seminar continued with a new session at the Romanian Police General Inspectorate.

As in previous year, pursuant to the seminars organized, the sites of the authorities responsible for Schengen acquis enforcement included special sections on personal data protection, communitarian and national legislation, information about the Supervisory Authority, informative materials issued by the Authority and the link to the Authority site.

On the recommendation of the Supervisory Authority, within the police, collectors were assigned as trainers for personal data protection and for the implementation of Schengen Convention and informative materials and flyers were produced. The trainees of the trainer courses organized in Campina and Bucuresti, where the Authority representatives also took part, gave vocational training courses on the topic of personal data protection.

Pursuant to the courses undertaken, the collectors' knowledge on the topic of personal data protection and Schengen issue was evaluated by assessment questionnaires disseminated locally and territorially.

One of the results of the information campaign initiated and supported by the Supervisory Authority is represented by the dissemination, through the TV network existing at the level of the police inspectorates, of informative materials about personal data protection and the duties of the Supervisory Authority.

Part of the international symposium ‚School and Family Violence Prevention' organized in Orsova in November 2008, a material about personal data processing by using video surveillance systems was presented.

The results of these actions were positive as the Supervisory Authority received many requests to organize vocational trainings to identify and solve the problems the collectors experience in observing the provisions of the framework law in the field of data protection; the points of view and information by phone requested by county inspectorates and other police structures increased as well.

Part 5: Cooperation with similar authorities of the European Union

In 2008, the Supervisory Authority representatives took part in the reunions of the working parties of Schengen, Europol and Eurodac joint supervisory authorities.

The main topics considered as part of these reunions dealt with: the Framework Decision regarding police and judicial cooperation in criminal matters, the bi-lateral agreements concluded by EU member states with third states on the topic of police and judicial cooperation and the data processing supervision performed by police authorities in the European information systems (Schengen, Europol, Eurodac, Customs). A very important aspect, considered in all surveillance activities, was the observance of the rights of the data subjects as part of the activity of data processing performed by the judicial and police authorities.

In April 2008, the Authority organized, by expert peers in Slovakia, an experience exchange on the topic of the correct enforcement of the personal data protection principles in Romania. The discussions considered the capacity and ability of the Supervisory Authority, in its quality of assessed institution, to accomplish its duties for the implementation of the provisions regarding data protection in Schengen acquis. On this occasion, a police precinct was checked, together with the border area between Romania and Serbia.

In the same context of assessment preparation, the Authority organized an experience exchange with the peer authority in the Czech Republic, in order to clear up some aspects regarding the Schengen assessment mission that the Czech data protection commission underwent in 2006: national legislation in the field, organizational structure, financial means allocated and financial independence of the Authority.

The collaboration with similar authorities in the European Union continued by the participation in international conferences - The Spring Conference of the European Data Protection Authorities organized in Italy, the Conference of Data Protection Authorities in Central and Eastern Europe - where the Supervisory Authority representative presented materials on the Schengen topic.

Part 6: The cooperation with the competent authorities in implementing the Convention for the enforcement of the Schengen Agreement

The collaboration between the Supervisory Authority and Schengen Department in the Ministry of Interior and Administrative Reform resulted, in 2008, in a collaboration protocol concluded between the two parties.

The main objective of this protocol is the preparation of Romania's accession to Schengen space, by observing the schedule approved in the field of personal data protection.

Based on the collaboration regarding the information campaign, the Supervisory Authority transmitted to IGPR and MIRA, for the purpose of territorial dissemination, informative materials about the rights of the data subjects as according to Law no. 677/2001, about the modality to exercise these rights and about the personal data processing according to the regulations in force: flyers, brochures, powerpoint presentations.

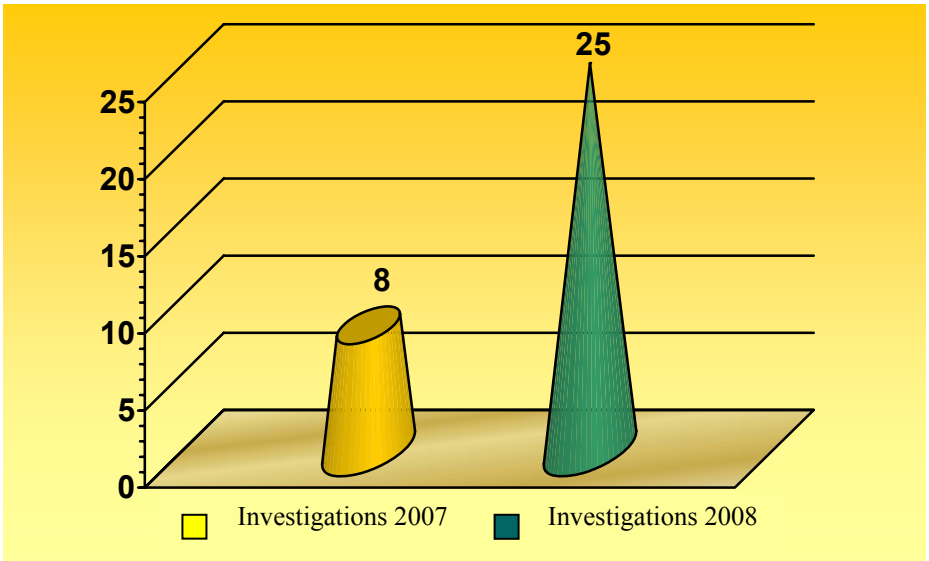
In 2008, on the Supervisory Authority initiative, a joint working party was set up, together with the representatives of the Ministry of Interior and Administrative Reform, the Ministry of Justice, the Ministry of External Affairs and of the Romanian Office for Immigration, in order to prepare the Schengen assessment in the field of personal data protection.

Reunions of the working party took part at the Authority headquarters; the reunions focused on the legislative adjustment of the data protection according to the communitarian acquis requirements.

Part 7: Investigations

According to the general investigation plan for 2008 regarding the preparation of Romania's accession to Schengen space - personal data protection and, with a view to meet the engagements undertaken, the Supervisory Authority checked the way in which Law no. 677/2001 is enforced by the controllers that activate in the police and in visa granting.

In 2008, *25 investigations* were performed, out of which 21 focused on police cooperation and 4 on visa granting.



7.1. Investigations that focused on the police cooperation

In 2008, out of the 21 investigations, 17 investigations were performed at the county police inspectorates, 2 at border police inspectorates and 2 at structures subordinated to the Ministry of Interior and Administrative Reform.

The investigations aimed at checking:

- the conditions for personal data processing by collectors

- the observance of the rights of the data subjects, according to Law no. 677/2001 and Schengen acquis,

- the expertise of the personnel involved in the preparation of Romania's accession to the Schengen space,

- the security measures implemented for the processed personal data protection.

Pursuant to the checks, the Supervisory Authority representatives recommended:

- to update the information transmitted by the notification forms,
- to inform the data subjects about all the processing performed,
- to fill in and transmit the annual activity report regarding the personal data protection,
- to update the work methods regarding the uniform enforcement of Law no. 677/2001 by the collectors,

- to create a special register for the requests to exercise the rights stipulated in Law no. 677/2001.

The most part of the checked controllers considered and put into practice the recommendations of the Supervisory Authority in due time and the Authority was informed about this aspect.

For the borders, the Supervisory Authority recommended that data subject should be informed on the rights they have, both in Romanian and in other languages, frequently used by the persons that come from states Romania has a common border with.

7.2. Investigations that focused on visa granting

In 2008, two consulates within Romanian embassies in third states and two structures subordinated to the Ministry of Interior and Administrative Reform were investigated .

The aforementioned investigations focused on checking the observance of the rights of the data subjects from the perspective of the national and Schengen acquis regulations regarding visa granting, the foreign citizens and asylum regime, the conditions for personal data processing, the expertise of the personnel involved in the personal data processing and the security measures implemented in order to ensure personal data protection.

The findings showed that the Supervisory Authority representatives made some recommendations for the Ministry of External Affairs collector.

CHAPTER V

THE REGULATION AND CONSULTATION ACTIVITY

The wide use of the personal data in all activity areas, as well as the progress of the informational technology suppose - a considerably data processing and exchange, so implicitly, a substantial growth of the cross boarder personal data flow between those implicated in the process, no matter of the public or private field in which they operate.

After signing the Convention no. 108, and subsequently after adopting the Directive 45/96/EC, the European Union Member States have sought to harmonize the internal legislation with the existent personal data regulations at the European Union level, but by being applicable to the national characteristics.

In order to accelerate the processes of implementing and harmonizing the national legislative of the acquis with the personal data regulations, applicable to different activity fields, the Supervisory Authority has constantly cooperated with the national institutions, by approving some legal instruments during their adopting process.

The Supervisory Authority has given a special attention to the problems raised by the data process done by some data operators acting in different fields and has intervened by regulations particularizing the personal data processing at the existent specific in some activity sectors.

At the same time, the Supervisory Authority has issued opinions, points of view, recommendations and instructions, according to the principles and provisions established by the European and national Acts applicable in the personal data processing.

Part 1: Legislative acts issued on grounds of Law no. 677/2001

During the year 2008, having in view the new status of Romania of member state of the European Union, the regulatory activity in the protection of personal data envisaged aspects found in the current activity.

Due to the Art. 29 Working Group recommendations of the existence of concordant practices with those of the European Union Member States and for the adequate application of the national legal frame, the following decisions have been adopted:

- ***Decision no. 90/2008 regarding an adequate protection level recognition in Jersey***

This decision was issued for the application of the European Commission Decision no. 2008/393/EC, adopted based on the European Parliament and by the European Union Council Decision 94/46/EC with regard to the processing of personal data and on the free movement of such data, referring to the establishment of an adequate protection level of such personal data in *Jersey.*

When adopting these regulations it had been taken also in consideration the fact that within the meaning of the Directive 95/46/EC, and also for the regulations regarding the protection of personal data existent in Jersey, this is considered to be a third country.

- ***Decision no. 95/2008 regarding the standard printed forms for the notifications Provided by the Law no. 677/2001 with regard to the personal data processing of and on the free movement of such data***

Considering the necessity of simplifying the internal notification procedure and that of avoiding the excessive administrative formalities, the Supervisory Authority has established a single printed form that will be used by the personal data operators starting with the 1st of March of 2009, instead of the two existing ones.

A supplementary argument in taking this decision has been constituted by the Working Party Art recommendations. 29, expressed in the Report no. 1227/2005 regarding the importance for standardizing and simplifying the notification procedure of the national surveillance authorities, as well as adopting some less costly methods for putting them in practice.

At the same time, the provisions of the Directive 95/46/CE have been considered, presenting the fact that the notification is destined to insure the purpose publicity and that of the main characteristics of the data process done by the personal data operators, so that the supervisory authority can control the concordance of the declared processes with the national legal provisions in the field.

- ***Decision no. 101/2008 regarding the issuing procedure of the authorization for personal data processing regarding the health state, in the conditions of the art. 9 paragraph (3) and (4) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data***

Issued in the application of the provisions of the art. 21 paragraph (3) letter c) reported at the art. 9 paragraph (3) and (4) from the Law no. 677/2001, this decision establishes the procedure based on which the Supervisory authority authorizes some data processing with regard to the health state, with the purpose of protecting the life, physical integrity and health of other persons than the data subject or of the public in general, in the situations in which the data subject did not consent in writing and in an unequivocal way.

This regulation is founded on the provisions of the Directive 95/46/CE, according to which the member states can derogate from the interdiction to process special data when this is justified by reasons of important public interest to some domains such a public health or health insurance. When applying these, through the art. 7 paragraph (2) from the Law no. 677/2001 with the subsequent amendments and additions, has been established the exception according to which the data processing regarding the health state can be done when the law expressively provides, with the purpose of protecting an important public interest, with the condition that the processing is done with respecting the data subject rights and also of the other warranties provided by the Law no. 677/2001.

The authorization model to be used in the situations governed by the above mentioned provisions has also been established.

Part 2 Endorsement of legislative acts

The supervisory authority shall be consulted on basis of the provisions of art. 21 paragraph (3) letter h) of Law no. 677/2001, when preparing legislative act projects referring to the protection of the rights and liberties of the persons regarding personal data processing.

Therefore, during the year 2008, there were basically endorsed the following legislative act projects:

- The project for the Government Decision with regard to the Elector Card Model
- The project for the Government Decision for amending the Government Decision 839/2006 with regard to the form and content of identity documents, of the sticker, residence establishment and of the register of tenants.
- The Project of the Government Decision with regard to the authorization procedure of the Public Service Providers of Public Authentication.
- The project for the Government Decision for amending the Government Decision 1085/2003 for applying some provisions of the Law no. 161/2003 with respect to ensuring some transparency insurance measures in exercising the public dignity, of the public functions in the business environment, the corruption prevention and sanction, referring to the National Electronic System implementation.
- The project for the Government Decision for approving the National Strategy with respect to joining the Schengen space for the period 2008-2011 and the Memorandum project with the theme: Approving the Schengen Action Plan 2008
- The project for the Government Emergency Ordinance for amending and completing the Law no. 19/2000 with respect to the public pension system and other social insurance rights, with the subsequent amendments and additions.
- The project for the Government Emergency Ordinance for amending and completing Government Emergency Ordinance no. 104/2001 with respect to the organization and function of the Romanian Boarder Police and the repeal of Chapter 4 of the Government Emergency Ordinance no. 105/2001 with regard to the Romanian state boarder.
- The project for the Government Emergency Ordinance for amending and completing the Law no. 290/2004 regarding the criminal record.

- The project for the Government Emergency Ordinance for amending and completing the Law no. 248/2005 regarding the free movement of Romanian citizens abroad
- Law Project for applying the international penalties.
- Amendment propositions of the Civil Procedure Code
- The Bulgarian Counter project of the Agreement between the Romanian Government and the Bulgarian Republic Government with respect to the police cross-border environmental cooperation in criminal matters.
- The Agreement Project between the Romanian and Hungarian Governments with regard to the cross-boarder cooperation in criminal matters. The law title has been modified after the negotiations with the Hungarian part in the Agreement of the Romanian Government and the Hungarian Republic Government regarding the prevention and fighting against the cross-boarder criminality.
- The Norm project for amending and completing the Norm no. 18/2007 with regard to the initial joining and evidence of the private administered pension fund participants, with the subsequent amendments and additions.
- The Law Project for ratifying the Agreement between the Romanian Government and the Hungarian Republic Government regarding the cooperation for the prevention and fighting against the cross-boarder criminality.
- The Understanding Project between the Work, Family and Equal Chances Romanian Ministry and the Federal Finance Ministry of the Federal Republic of Germany regarding the cooperation for combating the cross-boarder fraud in the field of work and social security contributions and undeclared work, as well as the cross-boarder hiring of working men.
- The Project for the Government Emergency Ordinance regarding the regulation of personal data use by the Police - transposition of the Recommendation no. 87 (15) from the 17th of September 1987 of the Committee of Ministers of the European Council.

From the 17th projects of legislative acts subject to the Supervisory Authority approval, only one has been favourably approved without any observation.

With regard to the text of the other legislative act projects, the Supervisory Authority has formulated observations and recommendations which have mainly been assumed by the initiating institutions, so that their final content, with the amendments and additions proposed by the Authority, has been favourably approved.

Among the observation approved projects, the following have raised special aspects:

- **Project of the Government Decision with regard to the authorization procedure of the Public Service Providers for Public *Authentication***

The Ministry of Communications and Information Technology has transmitted for approval to the Supervisory Authority the project of the Government Decision with regard to the authorization procedure of the Public Service Provider for Public Authentication. This regulatory act contains the provisions about the efficient access insurance of the citizens to public information and services, provided through electronic means by the public service providers of electronic authentication, and respectively by those juridical persons authorized, according to the law, to create and administrate the electronic identity for natural persons.

The Supervisory authority has remarked that, by processing the birth date and personal numerical code that will be transmitted to the consumer of electronic identity, an excessive personal data processing takes place.

Through the same project has been intended to introduce new control attributions for the Supervisory Authority.

But about this subject, the Supervisory authority has made some observations because their control attributions are established by the law, and not through regulatory acts with an inferior juridical force than that of the law, as are the Government decisions.

The Supervisory Authority observations have been taken into considerations, so that the Project of the Government Decision with regard to the authorization procedure of the Public Service Provider for Public Authentication, amended and completed, has been favourably approved by the Authority.

This project has taken the form of the Government Decision no 1129/2008.

- **The project for the Government Emergency Ordinance for amending and completing the Law no. 248/2005 regarding the free movement of Romanian citizens abroad**

The Ministry of Administrative Reform and Interior has transmitted for the final approval the project for the Government Emergency Ordinance for amending and completing the Law no. 248/2005 regarding the free movement of Romanian citizens abroad

About the transmitted document there have been formulated observations in accordance to the European Data Protection Supervisor Notice about the people age having the obligation to provide digital impressions, recommending that the age would be of minimum 14 years. Similarly, it has been determined that the age limit of 6 years present in the project has been established

without considering a solid and elaborated study as it is presented also in the European Data Protection Supervisor Notice from 26th of March 2008, published in JO no C200/1 from 6th of August 2008.

With regard to the principle of "one passport – one person" has been appreciated by the Supervisory Authority that this should be applied only to the children whose age is superior to the pertinent age limit (14 years) because the purpose of issuing a passport is that of facilitating the European citizens circulation.

Government Emergency Ordinance Project for amending and completing the Law no. 248/2005 regarding the free movement of Romanian citizens abroad has taken the form of the Government Emergency Ordinance no 207/2008.

- **The Agreement Project between the Romanian and Hungarian Governments regarding the cross-boarder cooperation in criminal matters, whose title has been modified after the negotiations with the Hungarian party in the Agreement of the Romanian Government and the Hungarian Republic Government regarding the prevention and fighting against the cross-boarder criminality.**

With regard to this Project, the Supervisory Authority has accentuated that "the special data" are the ones linked to the racial and ethnical origin, political, religious, philosophical and other opinions, trade-union belonging, as well as of the personal data of the health state and sexual life and that also the Directive 95/46/EC as well as the Law no. 677/2001 forbids the data processing, except foreseen express situations. Plus, it was considered to be necessary that the eventual dispositions regarding the special personal data processing to be introduced in the Vth Chapter of the Agreement project, named "Data protection".

At the same time, it has been appreciated in the context of the art. 6 of the Directive 95/46/EC and art. 4 of the Law no. 677/2001, that all the **characteristics of processing of personal data, respectively** the personal data making the object of parties transmission, to be adequate, pertinent, non-excessive, exact and actual, related to the purposes in which are processed.

Also it has been considered that the data can not be transmitted if there are reasons justified to suppose that in these way national legislations of the signatory countries of the Agreement or the subjects' legitimate interests would be broken. Moreover, if there are found incorrect transmitted data which are forbidden to be transmitted, the receiving data authority must be informed, this being obliged to immediately proceed at correcting or delete the data.

The Supervisory Authority has recommended that an article of the Agreement Project should be reformulated, so that the authorities transmitting and receiving the data are obliged to apply adequate technical and administrative measures for protecting the personal data against the accidental and illegal destruction, loss, modification or unauthorized access and disclosure, as well as against any other form of illegal processing, considering the provisions of the art. 17 paragraph 1 of the Directive 95/46/EC of the European Parliament and the provisions of the art. 20 from the Law no. 677/2001.

In the same situation it has been considered that the personal data can be transmitted, respectively disclosed to third parties only for accomplishing the purposes for which the data have been initially transmitted and that the authorities have the quality of data operators transmitting and receiving the data are obligated to hold the transmission and receiving personal data records.

About the persons' rights, it has been considered to be convenient that, upon request, to be offered information about it as well as the purpose of this data use, only if this information does not affect the prevention activities, research, criminal repression, research, criminal prevention and public order maintenance, as well as other activities in the criminal right, in the limit and restrictions established by law.

The Supervisory Authority has received for approval the final document, with the modifications made according to the transmitted observations.

The Agreement between the Romanian Government and the Hungarian Republic Government regarding the cooperation for the prevention and fighting against the cross-boarder criminality has been signed in Szeged at 21st of October 2008. Subsequent, the Supervisory Authority has received for approval the Project of the ratification Law of the Agreement between the Romanian Government and the Hungarian Republic Government regarding the cooperation in the prevention and fighting against the cross-boarder criminality.

- **The Project for the Government Emergency Ordinance regarding the regulation of personal data use by the Police - transposition of the Recommendation no. 87 (15) from the 17th of September 1987 of the Committee of Ministers of the European Council.**

Initially has been subjected for approval to the Supervisory authority a project of the Order of the Internal and Administrative Reform Ministry regarding the regulation of personal data in the police department, with the purpose of applying at national level the Recommendation no. 87 (15) from the 17th of September 1987 of the Committee of Ministers of the European Council.

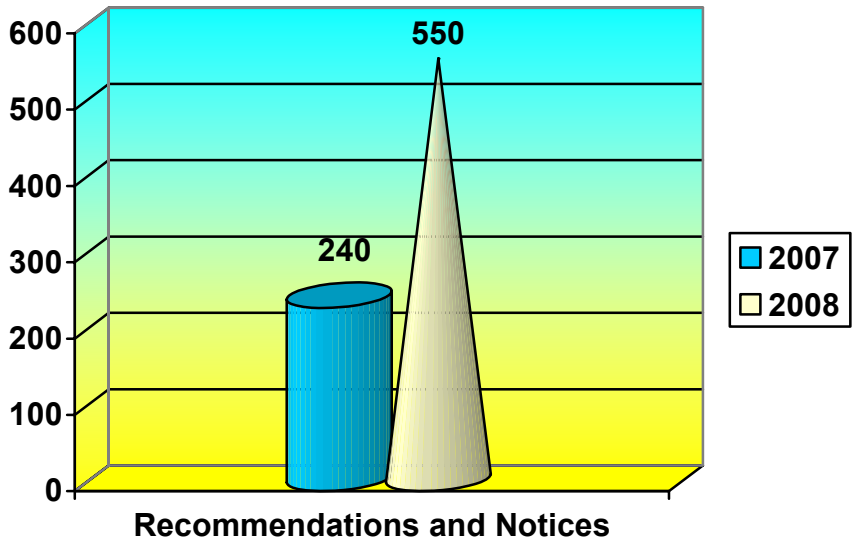
Because the implementation of the Recommendation is part of the Romanian obligations for harmonizing the national regulations with the Schengen acquis, the Supervisory authority has recommended its transposition in an emergency ordinance or law.

Accordingly, the Ministry of Administrative Reform and Interior has assumed our institution point of view and initiated the project of the Government Emergency Ordinance with regard to regulating the Use of Personal Data in the Police Sector.

The project has been favourably approved but with suggesting the modification of some dispositions referring to the personal data communication conditions towards the private sector entities, in accordance to the specific dispositions of the Recommendation no. 87 (15) of the Committee of Ministers of the European Council.

Part 3 Recommendations and Notices

The supervisory authority, based on the 21 paragraph (3) letter j) of Law no. 677/2001, formulates recommendations and notices upon any question linked to the protection of the fundamental rights and liberties of the persons regarding personal data processing.



1. In the year 2008, **9 recommendations** have been issued, of which we present the following:

- **Recommendation No 47/2008 towards the Justice Ministry**

The Supervisory authority has made a control for verifying the conditions for applying the Law no. 677/2001 and of respecting the security and confidentiality measures for personal data

processing by the Justice Ministry and National Administration of Penitentiaries for applying the Justice Minister Order no. 2856/C/2004 for approving the Regulation with regard to the constitution, organization and activity performance manner of the Discipline Commissions of the National Penitentiary Administration and subordinated units, amended and completed, and of the Justice Minister Order no. **2794/C/2004 for approving the deontological code of the penitentiary administration system personnel.**

Following the discovered things, the Authority has recommended to the Justice Ministry to take all the necessary measures for modifying the art. 38 of the **Regulation with regard to the constitution, organization and activity performance manner of the Discipline Commissions of the National Penitentiary Administration,** so that to ensure the abidance by the rules of the art. **5 from the Law no. 677/2001 according to which the personal data can be processed, including disclosed to third persons only if the subject data has expressly and unequivocal given her consent or in the cases established by the art. 5 paragraph (2) of the same regulatory act.**

- **Recommendation No 48/2008 towards the Romanian National Police**

The Supervisory Authority has been seized regarding a possible breach of the right to intimate and private life, by disclosing personal data from the register of tenants.

After the seized case clarifying investigation, it has been observed that the police units chiefs, as representatives of the Ministry of Administrative Reform and Interior, authority within whose territory the immobile is placed and for which they respond of the organization, guidance, functionality, updating and activity control of the register of tenants, as well as the training of the register of tenants responsible personnel, officially approved in this sense.

So, the Supervisory authority has issued a recommendation to the Romanian Police Department considering the investigation result and the provisions and principles established by the Law no. 677/2001, respectively of the non-excessive and legitimate of data processing, as well as the conditions of data disclosure, persons rights, including that of informing.

So, taking the necessary measures for realizing an efficient and homogenous training has been recommended for the immobile responsible from every police unit, including by issuing written instructions regarding the obligations due for respecting the provisions of the Law no. 677/2001, for personal data processing of the inscribed tenants in the register of tenants.

- **Recommendation No 61/2008 to a television channel**

The Supervisory authority made an ex officio investigation at a television channel for verifying the method of compliance of the Law no. 677/2001 in the campaign "Put your fingerprint!"

With this occasion has been concluded that a breach of the Law no 677/2001 can not be considered, because the collected data can not lead to identifying the data subject only by making considerable efforts in this manner, and the storage of tables containing personal data was done by a television channel without being organized in a determined structure dependent of some criteria permitting to process in an evidence system, as defined in the art. (3) letter d) of Law no. 677/2001.

With all this, the Authority has issued a recommendation to this television channel referring to adopting the personal data protecting measures, due to the special nature of the digital fingerprints.

For this, it has been recommended the destruction of all the tables containing personal data collected during the campaign "Put your fingerprint!" and then communicating to the supervisory authority the destruction protocol, signed by all the special users nominated for this operation, in a term of 5 days from communicating the present recommendation.

Likewise, it has been recommended to the television channel to exclude on the future the collecting data that are excessive and inadequate referred to their collecting purpose.

The channel has assumed the recommendations and transmitted to the Supervisory authority the stock taking and destruction protocol of the collected materials in the campaign "Put your fingerprints!".

- **Recommendation No 78/2008 to the Mayor of Sibiu City and Recommendation no. 79/2008 to the mayor of the village Piscu, Galati district.**

The Supervisory authority has received notices from different people, regarding the fact that at the local elections from June 2008, on local public authority level the elective lists have been posted outside the polling station, lists containing the personal numerical code, series and number of the identity document.

The Supervisory authority has investigated the raised issues and concluded that the processing, respectively the personal data disclosure through posting the elective list copies, does not respect the principles with regard to the personal data processing as is provided by the Law no. 677/2001 according to which the data destined to make the object of processing must be processed in good faith and according to the effective legal provisions, collected for determined purposes,

explained and legitimate, adequate, relevant and non-excessive referred to the purpose of being collected and subsequent processed, exact, and if is the case, updated, saved in a form that permits the identification of the persons, strictly on the necessary period and for the purposes for which the data are collected and are subsequent processed

Towards these findings, the Supervisory authority has recommended to the Mayor of the Sibiu City and that of the Piscu village, Galati district to take all the necessary measures that with the occasion of the local authority public and general elections, the elective copy lists would be consulted by every interested physical person, only for personal data, so that the third personal data processing is ensured.

2. The fact that some personal data operators inscribed at the surveillance authority, but also data subjects or third parties have solicited a considerable number of Notices referring to some aspects regarding the personal data processing, highlighting the emphasized interest for the data processing field, as well as the good faith in respecting the effective field legislation.

Among these, we present the most relevant points of view referred to:

- ***Processing personal data of the deceased***

In the attention of the Supervisory Authority has come the problem of applying the Law no. 677/2008 in the case of personal data processing of the deceased persons. This is the case for identifying the data disclosure of some deceased persons for the realization of an artistic document.

Referred to the personal data processing of some deceased persons, the opinion of the Work Party opinion, art 29, expressed in the Report no. 4/2007, through which it is appreciated that, although the personal data regarding the deceased persons must principally not be considered personal data based on the Directive 95/46/EC, because the deceased person does not have the physical person statute anymore, according to the civil law, and the data with regard to the deceased person can in some cases, indirectly benefit by a certain protection.

Moreover, the Working Party art 29 considers that nothing prevents a Member State to extend the application of the national legislation regarding the personal data protection to other fields than that regulated by the Directive 95/46/EC, with the condition that these are not contrary dispositions to the community law.

With regard to the case submitted in the attention of the Supervisory Authority, the Law no. 677/2001 provides that, if the data processing is done exclusively on journalistically, literary or

artistic purposes, this can be done without the consent of the person in question, with the condition that the respective data to have been disclosed by the person in question, or to be closely related by its public person quality of the data subject or by the public character of the facts in which that person is implicated. If these legal conditions are not complied, is necessary to obtain the consent of the data subject.

So, the Supervisory Authority has considered in the same sense as the Work Party Art. 29, that the personal data of deceased persons can, pursuant, in some cases, indirectly benefit by the same conditions as the data of live persons.

- ***Processing personal data of the under aged persons***

With regard to the under aged persons personal data, the Working document no 1/2008 is remarked, with regard to the under aged person's personal data protection, issued by the Work Party art. 29. This document highlights the new applicable principles to the under aged data processing, respectively, the superior interest of the child, his protection and care, the right for respecting the under aged private life, his rights to be represented, the adaptation of the maturity degree of the under aged and not in the least his right to be consulted.

According to these principles, as well as the general ones applicable to the data processing, the Supervisory Authority has expressed its opinion every time the operators' preoccupation from the private law field for the under aged protection has been put across in the solicitations addressed to the Authority.

So, with respect to the obtaining conditions for the consent of the legal representatives of the under aged participants to promotional campaigns organized by operators, has been highlighted the fact that the personal data collecting operations of the under aged through the internet are susceptible of presenting special risks for their rights and liberties, reason for which is necessary that the operator have in view the insurance of effective protection for the under aged.

For clear information of the data subjects – in this case the under aged – when collecting the data through electronic forms, the operator mush provide in their near proximity, together with minimal information, supplementary information through the complete text of the contest rules by putting an internet link towards it. Therewith, it has been specified that is necessary to integrate in the contest regulation provisions referring to the consent procurement modality of the legal representatives of the under aged regarding the personal data processing and use.

As the personal numerical code, series and number of the identity documents of the legal representative of the under aged collecting is concerned, the Supervisory authority has highlighted that, constantly, this must be done according to the provisions of the art. 8 from the Law no.

677/2001 corroborated with respecting the principles of data necessity and purpose proportionality established by art. 4 included in the same law.

The Supervisory Authority has appreciated that, depending of the child's age, data would be solicited from the child's legal representatives – like contact data (phone number, e-mail address, etc) in order for this to be contacted, or the contests signing up of the under aged can be conditioned by the parents' consent, by providing the free phone number (Like a *green call*) where supplementary information regarding the purpose of processing or transmitting a document to the parents to be signed can be offered (classic or with electronic signature). In these situations, the way from which it results the fact that the under aged' legal representative are giving their express and unequivocal consent must be chosen so that its evidence can be provided, in case this thing is imposed and to exist the certainty of its origin.

In the same manner, a commercial company has asked the opinion of the Supervisory Authority regarding the posting conditions on the contest' internet site, the participants' photographs, among these being also under aged.

In which concerns the under aged between 14 and 16 years old, to which the law recognizes a limited exercise capacity, their agreement and their legal representatives consent are necessary.

Related to this aspect, the legal provisions guaranteeing the children' rights about protecting their public image, intimate, family and private life as well as the protection against other exploitation form, abuse, etc must be taken into consideration.

The Authority specified as supplementary protection measure the necessity of avoiding the association of the image with the name, first name and the minor' age when posting their photographs on the Internet. This measure can be taken for all the contest participants, and about the data saving period (especially of the image) it was recommended that this be strictly established to the necessary period for realizing the purposes for which this have been collected and subsequent processed.

It has also been highlighted the fact that the electronic forms must contain only the necessary data destined for completing the purpose and all the security measures destined to guarantee their confidentiality must be ensured, and if it is obligatory, the forms will specify the compulsive or optional character of data provision.

As posting other persons' image is concerned (friends of the contest participant) on the site, this is an indirect personal data collecting method. In this situation, the operator must ensure that the persons in question know the identity of those providing the image and have provided their express and unequivocal consent for their data processing.

- ***Processing of personal data in systems like the credit bureau type***

The Supervisory Authority opinion has been asked regarding the established condition in the Decision no. 105/2007 with regard to the personal data processed in credit bureaux type systems, referred to the existence of a written agreement of the data subject - necessary for transmitting the personal data to the Credit Bureau, in order to be checked by interrogating/consulting the evidence system owned by the Bureau.

The mentioned decision states that the credit solicitors' data are transmitted to the Credit Bureau, the purpose being that of evaluating their reliability, in order to offer the loan.

Due to the fact that the respective regulation solicits the written agreement of the data subject, obtaining it online is valid only with the electronic signature implemented according to the law or through other identity confirming methods Contrarily, there is no certainty about the credit solicitor's identity, and when it's imposed, the written agreement certain evidence can not be provided.

If during these procedures, the personal numerical code is being also collected in order to realize a preliminary analysis of the applicant's eligibility for the credit, in supervisory authority's opinion expressed in different situations, the discussed processing is excessive in report to its purpose, breaching the principle from the art. 4 from the Law no.677/2001. The personal numerical code data or of other personal data having general application identification function can be done only if the data subject has expressively given its consent or the processing is expressively provided in a legal disposition.

In the case of Personal Numerical Code, the online personal data collecting system must ensure the express and unequivocal attainment of the data subject' consent, as well as offering adequate guarantees for respecting the data subject rights; in this manner, the personal data processing is done by taking the necessary measures for ensuring the data security processing.

With regard to the online interrogation of the Credit Bureau with the purpose of preliminary analysis of the potential clients' eligibility of the bank, the Supervisory Authority has stated that such a measure is not grounded because adequate guarantees can not be instituted for respecting data subject' rights.

Moreover, the Supervisory authority has pointed that, through the web application, just a preliminary evaluation and not an actual approval/rejection of the credit is done, and so it considered that in this phase the data base interrogation of the Credit Bureau in order to check the applicant is not necessary.

- ***Processing of the personal data in the case of overseas transfers***

The Supervisory Authority has been solicited to express its position regarding the data transmission belonging to natural persons to the country's embassy in Bucharest.

By respecting the community principles stated in the Directive 95/46/EC in the Law no. 677/2001 a series of rules and exceptions regarding the overseas data transfer have been established, and mainly the principle according to which, the Member States will permit the transfer only if the destination states to which the data are transferred ensure an adequate protection level of the personal data.

Has been stated that, besides the general rules for the personal data overseas transfer, there are exceptional situations in which the transfer is permitted even if the destination state does not have an adequate data protection level, and if the situation meets one of the conditions established by law, the data transfer can take place.

The Supervisory authority has appreciated that the solicited data can be transmitted only with the data subject' consent.

- ***Personal Data Processing using Video Surveillance Means***

The purposes of using the video surveillance systems are, mainly, those of controlling the moving of people and goods, access in some spaces, access to some events and situations, as well as the employees' access in the working place and that of monitoring the correctness and efficiency of their activity.

In this context, the Supervisory authority has been solicited to give its opinion regarding the legitimacy of using by an employee from an autonomous administration., the recorded material containing images regarding fuel stealing from the motor depot as evidence.

It has been mentioned that the Law no. 677/2001 regulates the sanctioning regime of the contravention acts done by personal data operators regarding the personal data processing.

Referring to the presented aspects, the Supervisory authority appreciated that the act is included in the crimes against the patrimony category, incriminated and punished by the Criminal Code, and so the Law no. 677/2001 does not apply, and the Supervisory authority is not competent in this situation and, lesser in establishing the legacy and relevance of the recorded material as evidence.

The Supervisory authority pointed out that, according to the opinion of the art 29 Working Group. with regard to the data processing used in the hiring cases, and the fact that the video surveillance of the employees can be done by the employer by respecting the legal provisions and

also by consulting, if it is the case, of the employees representatives and those of the trade unions. The video surveillance purpose must be determined, explicit and legitimate and the data must be adequate, pertinent and non-excessive by reference to the purpose. The data can only be processed in good faith and according to the legal provisions and must be stored during the period necessary to accomplish the purpose of their use, by ensuring the data subject' rights, especially those of information and if the situation imposes it – obtaining its consent.

The recorded images using the surveillance methods installed in the legal conditions mentioned above can be disclosed to the police departments in order to perform a criminal investigation.

As for the installation of hidden surveillance cameras, this procedure is forbidden, except as provided by the law and with the competent organ' authorization.

- ***Data processing through call – centre services***

Often situations in which economic agents, with the purpose of improving their specific services, proceed at recording the clients' telephonic conversation, by presenting a welcoming message are lately met.

The Supervisory Authority opinion has been asked regarding the manner of obtaining the telephone users' consent or by registering telephonic conversations.

The dispositions of the Law no. 506/2004 states the conditions to be respected in order to ensure the communication confidentiality, as well as the exception cases in which hearing, registration, saving or any other communication or data traffic intercepting or surveillance is permitted.

Related to the legal provisions, the presented purposes in the greeting message used by the respective agent, the Supervisory authority appreciated that the method for obtaining the consent – through the registration of the telephonic conversations with the client respect the provisions of the Law no. 506/2004.

The Supervisory authority stated that, if there are cases in which the data collection includes data or sensible data categories, for which the Law no. 677/2001 imposes to obtain the written consent, the above-mentioned method can not be accepted.

As the information of the data subject done according to the general provisions established by the Law no 677/2001 is concerned, the Supervisory authority appreciated that also the special provisions of the Law no 506/2004 must be taken into consideration; respectively the subscriber or user must be given the possibility to refuse the saving or the access to the stored information. The Supervisory authority recommended that the information should include also references to the

refusal consequences of the person in question to accept the provision of personal data in this manner and the possibility to appeal to alternative methods.

Part 4 The activity of representation before courts of law

During the year 2008, we observed that the courts of law adopted a unitary practice in litigations regarding the protection of data.

Following we present some relevant situation in which the applicable penalties by the Supervisory authority have been disputed.

1. After the investigation done in a limited responsibility company, the authority has found that the company processed personal data through the electronic mail. For the operator's act, a contravention fine has been applied for transmitting unsolicited commercial information through electronic means. The operator followed a complaint against the finding/sanction report.

Taking into consideration the cause probative, the court found that the operator processed the clients' personal data, including through commercial messages transmission, without offering the receiver the opportunity to exercise his opposition right. So, the receiver was repeatedly receiving unsolicited commercial messages, without him giving his prior consent.

In these conditions, the court has decided that the contraventions provided in the art. 13 from the Law no. 506/2004 have been well applied by the Supervisory authority, and the fine has been legally applied.

In pronouncing the decision, the court has retained that the Supervisory authority has applied the contravention penalty respecting the provisions of the Government Ordinance no. 2/2001 with regard to the proportionality between the given contravention penalty and the social danger degree of the committed contravention act.

Analysing the presented arguments by the Supervisory authority, corroborated with the effective legal provisions, as well as with operator's reasons, the court has rejected the complaint as being ungrounded.

2. In the field of personal data processing by using video cameras, the Supervisory authority has investigated at a personal data operator, where was a breach in the obligation to notify the authority; this is considered a contravention act, incident to the Law no. 677/2001.

The image constitutes indubitable a personal data because can lead to identifying the person in question. Besides, the Directive 95/46/CE established that the images have a personal data character.

The operator had installed video surveillance cameras in order to process the persons' image, sustaining that, from his point of view, the image is does not have a personal data character, so this can be processed without being incident to the Law no. 677/2001.

For the determined contravention act of this operator, the Supervisory authority has applied the contravention penalty, as provided by the law.

The operator has disputed the finding/sanction report, but the court has rejected the complaint as groundless, consenting that, the Supervisory authority has applied the penalty correctly and legally, according to the provisions of the Law no. 677/2001.

Not satisfied by the court given sentence, the operator has subjected an appeal against it. The Court of Appeals Bucharest has rejected the appeal as groundless.

Consequently, the Supervisory authority has applied the sanctions according to the effective legal provisions.

3. During a sport club investigation, the Supervisory authority has found that the agent was manually and automatically processed the personal numerical code, first and last name of the supporters buying the subscriptions, without a prior notification of processing these data and without informing the persons in question regarding their lawfully rights.

Also, has been sustained that in the finding/sanction report the contravention acts were not inscribed, as well as the fact that the execution date was not mentioned, although the report data was present and the contraventions had a continuous character.

The Supervisory authority has sanctioned with a contravention the operator for omitting to notify the supporters regarding their personal data processing, as well as for not informing the persons in question about the lawfully rights and processing conditions.

Pursuant to the sanction, the operator has notified the authority about the already done processings and informed the data subjects about their rights presented in the Law no. 677/2001.

With regard to the complain object formulated by the operator, the court has decided that "the facts retained as contraventions are continuous acts, situation in which the data of the report represents the data of their breach."

Consequently, the Authority's findings and procedure have been correct and the court has maintained the sanctions applied by our institution.

4. After receiving a complaint, the Supervisory authority has made an investigation in a bank where the illegal personal data processing has been discovered, by breaching the provisions of art.14 and art.17 within Law no. 677/200; respectively ignoring the right intervention and that of not being submitted to an individual decision.

So, for the contravention act done by the bank, the sanction provided in the art.32 from the Law no. 677/2001 has been applied.

The Bank has contested the finding/sanction report, motivating the insufficient description of the act, as well as the fact that the petitioner's data transmission to the Credit Bureau was done as consequence of a technical error in the informatics' program.

The Credit Bureau data transmission was done without informing the person about this operation, although he previous paid for the credit.

The court has rejected the bank's complaint as groundless

In giving the sentence, it has been taken into consideration that the operator has recognized his act - constituted in the existence of a technical error in the informatics program, leading to a wrong report of the petitioner to the Credit Bureau, in the presented complaint, as well as at the time of concluding the finding/sanction report.

In conclusion, we underline the fact that, besides the variety of court complaining aspects and situations submitted to the court's control, the interpretation of the personal data legislation was done by the court in a similar manner as the one proposed by the supervisory authority.

In this context, special mention must be made on the interest shown by the magistrates to the conditions of the processing of personal data, resulted in the organization with the Superior Council of Magistracy of symposia with specific content in which some aspects of the practical appliance have been approached.

CHAPTER VI

ACTIVITIES IN THE FIELD OF INTERNATIONAL RELATIONS

In the accentuated personal data processing diversity context which are done in an extreme variety of international fields (Internet Technology, RFID, passengers, biometric, health, fight against criminality and especially anti-terrorism data processing), a special attention to these aspects and to follow the legislative European evolutions it is imposed.

An important component of the Supervisory Authority international activity is monitoring the European Union legislative evolution and formulating some legislative modifications in order to harmonize the national legislative framework with the community one. The European evolutions have implied the participation and contribution transmission in the inter-institutional groups organized at national level on specific activity levels (consumer protection – TESTA, police and juridical co-operation, airline passenger data processing).

Besides these, the international relations co-operation activity includes also transmission of points of view, opinions, presentation of some specific cases met in the current Supervisory Authority' activity, filling and transmission of forms on specific domains, received from European organisms (European Commission, Union Council and Council of Europe) and similar authorities of other states and non-governmental organizations.

Part 1: International level working groups

The Supervisory authority has also taken part in the year 2008 at the most important working platforms existent in the personal data processing at international level, like: Art 29 Working Group JSA Schengen, JSB Europol, JSA Customs, Eurodac, Working Party on Police and Justice, Advisory Committee of the 108 Convention and the International Telecommunication Working Party.

1.1. Art 29 Working Group 29

In over 10 years of activity, the Art.29 Working Group created on the grounds of Directive 95/46/EC, has become one of the most important co-operation organism in the data processing field, in which a variety of topics with legal and technical implications have been put into discussion.

Among these we remind the ones dominating the activity of the Working Group in 2008. Data transfer to third countries (Binding Corporate Rules – BCR and Passengers Data – PNR), underage personal data protection, telecommunications and new technologies.

Data transfer abroad

As a continuation of the efforts done in 2007 with respect to the procedure changes for speeding up the adoption of the procedures regarding the existing obligatory rules in the data transfer abroad operated by companies and corporations („Binding Corporate Rules"), in the year 2008, the Working Group has adopted three important documents.

The first of these documents adopted in June 2008 established the frame for the „Binding Corporate Rules" structure. A few years ago, the Working Group has adopted a series of documents establishing the fact that the data transfer from the European Union in a corporation can take place only based on the „Binding Corporate Rules"; has also elaborated a guide about the elements that must be contained by these binding rules.

During the June 2008 plenum, the Art.29 Working Group has adopted another document establishing the elements and principles that must be found in the „Binding Corporate Rules".

A third document regarding "Frequent questions" linked to the „Binding Corporate Rules" has been adopted in October 2008. In its content, the Art 29 Working Group iterates the fact that the

„Binding Corporate Rules" represent a proper solution for the multinational companies to respect the legal obligations and ensure an adequate level of personal data processing which are transferred outside the European Union.

The Working Group has adopted this document starting from the Data Protection Authority experience regarding the forms presented for approving the „Binding Corporate Rules". Also, through the "Frequent question" (FAQ) document, clarifying some specific requests to be fulfilled by the data transfer solicitors of the authorization outside the European Union is followed, so that they obtain the approval for the „Binding Corporate Rules".

Passengers data processing (Passenger Name Record – PNR)

An aspect to which the Art 29 Working Group has given a special attention during the year 2008, was the passengers' data processing.

In June 2008 the Opinion no 2/2007 regarding the information of passengers regarding the PNR data transfer to the authorities of the US. This opinion is addressed to the Travel agencies, airline companies and other organizations offering transport services to the passengers travelling to and from the US.

Presently, the legal framework for the PNR data transfer to the US authorities is the Agreement signed in July 2007 between the European Union and US. Informing the passengers regarding the personal data processing is the responsibility of the travel agencies and of the airline companies.

The above-mentioned Opinion clarifies aspects regarding who must present the information and also what, mode and moment of the information must be provided. In the Opinion attachments, the Wording Group has elaborated notices models for facilitating the necessary information provision to the travel agencies and airline companies and, also to ensure that the provided information are valid for the entire European Union.

The National Personal Data Supervisory Authority ensured the participation of the subgroup's reunions, their representatives being actively implicated for making numerous materials. Due to this contribution, mid 2008, Romania, through the Supervisory authority, has been nominated to be vice-reporter in the Passengers Data Processing subgroup (PNR).

Under aged protection of personal data;

The analysis started in 2007 regarding the mode in which the under aged personal data are protected, has taken effect in 2008 by the Working Group adopting the document regarding the under aged personal data protection. Being an extensive department, the Art 29 Working Group has concentrated in this document upon the under aged personal data processing inside the teaching units because the processed data have usually a sensitive character.

In this manner, the document is addressed to the teaching units' professors and also to the data protection authorities who are responsible for supervising under aged data processing in schools. The purpose was to identify the important legal aspects regarding child data protection and generally offer a guide to those working in this field.

The Internet and the new technologies

Admitting the utility and importance of the search engines that have become a component part of the everyday life of people using the Internet and the information searching technologies, the Art 29 Working Group has adopted in April 2008 the Opinion on data protection issues related to search engines.

In the content of this Opinion, the Art 29 Working Group identifies a series of responsibilities of the search engines providers - as personal data operators; the main objective of this adopted document was that of establishing an equilibrium between the legitimate commercial necessities of the search engines providers and the personal data protection of Internet users.

Among the approached aspects in this document is also the definition of search engines, categories of data processed for providing search services, legal framework, processing purposes, informing obligation of the persons in question and also of their rights.

The main conclusion that can be drawn from this opinion is that the personal data must be processed by the search service providers only by having legitimate purposes.

1.2. Common supervisory authorities in the police and juridical co-operation field

In view of the Romania's preparation of acceding to the Schengen Space, as well as in virtue of the European Agreements in the police and judicial co-operation, the Supervisory authority has actively participated at the activities involved by the common control authorities founded in this specific co-operation field – JSA Schengen, JSB Europol, JSA Customs, Eurodac and Working Party on Police and Justice. The supplementary information about these aspects are content in the "*Chapter IV – Preparatory activity for the Accession to the Schengen area* „

1.3. *The Consultative Committee of the Convention no 108/1981 for the protection of persons regarding the computerized processing of personal data and the Office of the Consultative Committee of the Convention no.* ***108 (T-PD and T-PD-BUR)***

The T-PD activity focused on the "profiling" activities supposing the profile setting - behavioural and of other nature, of a person or a group of people, after „processing" a group of information referred to them, including personal data of the persons in question. This type of activities used initially by the police authorities with the purpose of identifying the criminals, are

frequently founding new applying domains, especially in promoting and selling different products, depending on the buyers financial possibilities, or of other information regarding them.

Another very important aspect in the T-PD activity was the Committee's implication in elaborating, in co-operation with the World Anti-Doping Agency of an International Standard for the personal data processing protection during the organization' activities. The main role of this International Standard is that of ensuring the warranty, by the organizations and persons implicated in the sports anti-doping fighting activities, of an adequate protection level of the personal data processing, no matter some specific national provisions in the field.

1.4. The International Working Group regarding the Protection of Data in Telecommunications

Another important platform is the International Working Group regarding the Protection of Data in Telecommunications Among the aspects discussed within this group, there are: Data processing within the registration devices existent in vehicles , personal data processing within the Google services and of other search engines, implication of applying the Convention no. 185 with regard to the cybernetic crime against the private life, international standardization and private life, biometric encryption and private life, saving the SMS content, with the purposes of applying the law.

During the last part of the 2008, due to the financial Government restrictions, the Supervisory authority could not respect its participating commitments to the working groups and subgroups organized at European level.

Part 2 The collaboration with other supervisory authorities

Taking into consideration the necessity of preparing the Schengen evaluation mission for the data protection field, for which the supervisory authority will be evaluated and which will take place in April 2009, during the year 2008 exchanges of experience on the Schengen problematic have been done with the Czech and Slovakian Data Protection Authorities. The two supervisory authorities have been previously evaluated and, based on their own experiences, have provided to the Romanian Supervisory Authority a series of relevant information for the 2009 evaluation preparation.

Part 3 International Conferences

Also in 2008, the supervisory authority personnel have participated at a series of conferences, European and international seminars which were considered to be important from the approached subject perspective. Among these, we mention:

- Conference Data Protection Authorities of Central and Eastern Europe (Poland);

- The XVIIIth Meeting of the Casuistry Seminar (Slovakia)
- Spring Conference of the Data Protection Authorities (Italy)
- International Conference of the Data Protection Authorities (France)

Attending these events, the Romanian supervisory authority representatives have presented materials with different topics, like: “The National Visa Policy", “Supervisory authority attributions in relation to the Police structures”, “Data protection within preparing the Schengen evaluation mission framework”.

Within the Casuistry Seminar which took place in Slovakia, a Romanian Supervisory authority representative has presided the session dedicated to the video surveillance.

Likewise, with the occasion of the international reunion, general and specific activity reports have been transmitted and sustained.

CHAPTER VII
COMUNICARE ŞI RELAȚII PUBLICE

Part 1: The Communication and Public Relation Activity

Also in 2008, the development of the communication activity represented one of the essential components of the supervision authority.

The Supervisory Authority has been involved in a series of national specific activities with the purpose of increasing the public’s informing and realizing of the personal data protection field.

So, more reunions and round tables within the authority’s office have been organized with the participation of some personal data operators from different activity fields and continued to inform at national level, with the support of the **prefect's institution and of other public authorities.**

Among the international events in which the Supervisory authority has been implicated in sustaining and publishing some works in close collaboration with the university environment, we mention:

- The International Conference “Realities and perspective of the European Integration process in the globalization era", organized by the "Lucian Blaga” University of Sibiu, within which

an analysis called “Aspects regarding the personal data processing in the criminal right field” has been presented.

International Conference “Business field criminality” organized by the Agora University of Oradea where the theme work “Unsolicited commercial messages – stringent reality of the contemporary informatics society” has been presented.

- International Conference “Credit Bureau – an important factor of a healthy credit activity” where the theme work “Information right in the financial banking sector” has been presented;

Among these manifestations pursue to increase the informatics’ level among the students and youths in general; the Supervisory authority has been also implicated in preparing the future ***specialist who will develop their activity in the Romanian Consulates***, by sustaining periodic lectures. ***The invitations received from the Training Centre for Consular Personnel from the Ministry of Foreign Affairs reflect*** the more intense preoccupations manifested in the contemporary society with regard to respecting the personal data processing principles.

At the beginning of 2008 a new website of the Supervisory authority has been done, in order to improve the modern communication, informatics and dialogue demands.

Through this the insurance of adequate information of the natural persons has been intended, as well as that of the operators soliciting for the authority’s opinion, including using the e-mail address put at their disposal: anspdcp@dataprotection.ro .

Along 2008, over 10.000 brochures referred to the main attributions of the Supervisory authority have been edited, as well as 4.700 folding about the notion of personal data and citizens rights, specific to the data protection field.

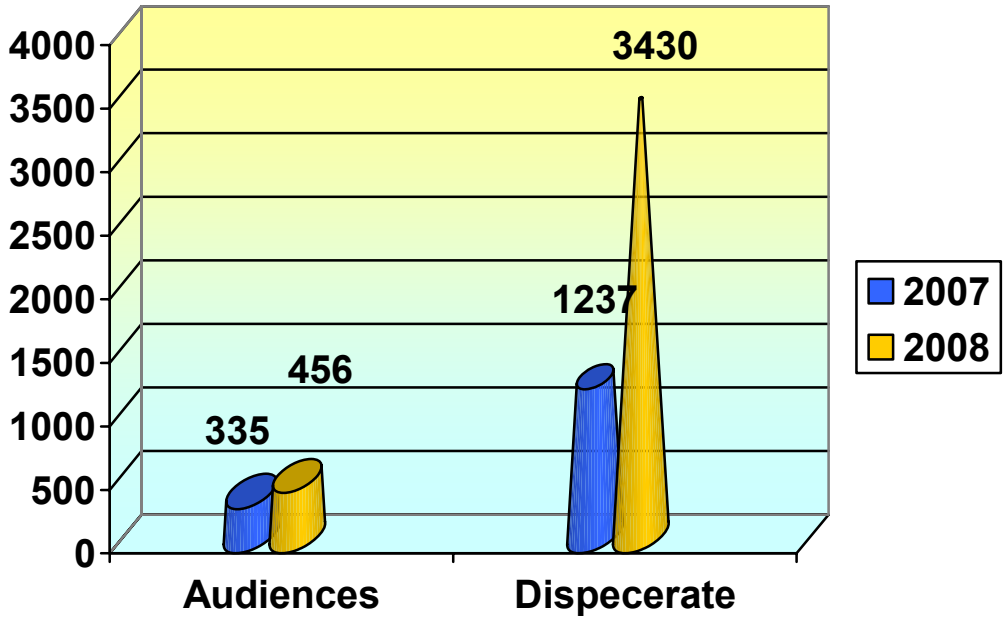
With the occasion of the European Data Protection Day, a brochure, one folding and one poster of this event has been made, for marking the importance of this day on the European plan. The informative materials have also been edited in English, being permanently available on the Authority’s website and office, in the space destined to the public audiences.

The Supervisory authority has continued also in 2008 the information of professional associations regarding their members’ obligations, including that established in the professional associations’ duty of elaborating the Code of conduct containing the adequate norms for the persons’ rights protection of whom the personal data are being processed.

The complex banking activities, data processing by this institutions of a significant personal data number and that of sensitive data including, has raised important problems about the elaboration of the “Romanian Banks Code of Conduct with regard to personal data processing".

By means of the dispatch and audiences services, a rapid and efficient information of the citizens and operators has been done, with the sense that have directly been provided useful

information regarding the in question persons rights and specific obligations of the operators, and also clarifications regarding the data processing conditions and their disclosure to third parties.



The personal data processing evidence register is opened for public consultation, according to the art. 24 paragraph (5) from the Law no. 677/2001, being available starting 1st of October 2008 and on-line.

Along 2008, a significant increase of this register consulting solicitations number has been registered, through e-mail and also mail, soliciting information about the operator quality of some commercial agencies or public authorities.

In this manner, the Supervisory authority has received in 2008 a number of 550 solicitations, soliciting information about the Law no 677/2001 application. Among this, a number of 365 have been transmitted through e-mail and for their rapid solving, the answer has been given in the same manner.

The main solicited aspects through these solicitations were - clarifying the operator quality or mandate of some companies with different activity objects, of some public institutions, operators' obligations including those of security and confidentiality insurance of the data processing, data processing conditions and their disclosure to the thirds, personal data transfer abroad.

***Part 2* The relationship with the mass media**

Along 2008 the data protection fields has constantly been in the media attention. The field of the protection of data was reflected in various radio and TV published press articles on different

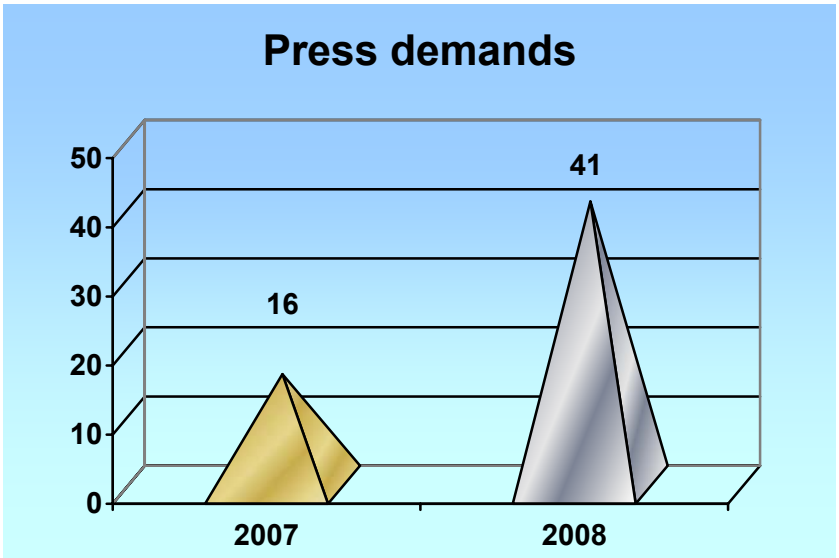
specific themes, aspect which demonstrates the growing interest of the mass-media for the specific issues of this field.

In this manner, the Supervisory authority representatives have been invited to numerous shows broadcasted by public and private radios and televisions, where main aspects of the data processing protection activities have been presented (TVR 1 and 2, Antena 1, PRO TV, Radio România Actualități, Radio Oltenia).

Other radio stations, such as BBC broadcasted the point of view of the representatives of the authority with regards to aspects regarding personal data use conditions in credit bureau record systems.

Along the whole year, the written press reflected the activity of the Supervisory authority in various articles highlighting diverse aspects, through articles published in the national press (Curierul Curierul Național, Săptămâna Financiară, Cotidianul, Adevărul, Jurnalul Național, România Liberă, Gândul), as well as in the local one, including by the financial information sites. (*www.**hotnews**.ro*, *www.**bizcity**.ro*).

The written press solicitations have significantly increased in 2008 in comparison to the last year.



In some of these materials the importance of the data protection field at European and national level has been presented, citizens' rights in this field (especially the right of complain and information), exploiting possibilities and the role of supervisory authority. Other materials have emphasized on the means the Supervisory authority disposes for sanctioning the operators breaching the legal provisions in the field and also ensuring the data base security by each operator.

Along 2008, the authority representatives have sustained press conferences with the occasion of local reunions. With these occasions, information about the supervisory

authorities' activity has been provided to the press, of the legal regulations in the field and the taken measures along the investigations and controls.

With the purpose of making known the activity of the institution and the specific regulations in the field, there were disseminated 25 press releases on the www.dataprotection.ro site, by which significant aspects from the authority' activity, information campaigns and manifestation of the authority or through which some normative decision projects have been put for public consultation. Some of these have been transmitted to the main press agencies.

CHAPTER VIII

MATERIAL RESOURCES CONSUMPTION AND ASPECTS REFFERED TO THE 2008 BUDGET

For the year 2008, the institution had funds allocated through the State Budget Law no. 388/2007, with the subsequent amendments and completions, the final structure being the following:

Indicator name	Code	Updated budget on December 31st 2008	Spent amounts until December 31st 2008	Execution (%)
Total expenses, from which:		4.610 thousands lei	4.490 thousands lei	97,4 %
Staff costs:	10	2.934 thousands lei	2.921 thousands lei	99,6 %
Goods and services	20	1.469 thousands lei	1.364 thousands lei	92,9 %
Capital expenses	70	207 thousands lei	205 thousands lei	99 %

The existent restrictions on the budgetary execution have imposed a permanent updating of the priorities for the realization of the most important projects with the existent funds.

The limitation of opening credits starting with February 2008 has clogged the institution directors' mission who, in collaboration with the Human resources and economic direction, had to take the most efficient decision for ensuring the necessary material resource, framing them in the limits established by the Ministry of Economy and Finances.

So, as in the previous year, the imposed restrictions had as effect the renounce at goods acquisition and also of some investments.

As the allocation funds use is concerned, we can mention the following:

The Personnel costs of the authority constituted a percent of 63,64% of the total credits distributed from the state budget, of which an effective number of 2.921 thousand credits have been used. The majority of personnel cost related to the payments were done for the employees' work from the speciality departments. Due to specific conditions regarding the continuation of authority operations pursuant to Romania's integration to the European Union, some activities have been done including outside office hours; in the employees paid amounts is also included the payment of supplementary hours that can not be recuperated through free time in a time of 30 days.

Hereinafter, due to the insurance impossibility of an office from the state patrimony, the rent costs have been an important part (46%) from the total goods and services costs, as well as from the total budget funds used in the year 2008 – 14%.

The travel costs represented a number 6.2 % of the 2008 total cost. Must be mentioned the fact that the supervisory authority realizes its main activity objection through investigations and controls at operators situated along Romania, and also to the Romania's consulates.

At the European Union level, the Supervisory authority has the obligation to participate at the works of the Art 29 Working Group functioning next to the European Commission, as well as those of the working groups of the data protection field level, at the common control authorities works (Schengen, Europol, Eurodac) and at the European Council's works in the data protection field. So, the amounts allocated for travels include also all these expenses.

The relatively low level of other goods and services acquisition costs is the result of more factors, among which we mention: the lower price criteria applied to the acquisition procedures, together with some carefully established technical demands, as well as budgetary restrictions.

The budgetary execution afferent to the investment costs were of 99%; the following factors having influences upon this type of expenses: quarterly fund allocation, opening credits' monthly level, existent interdictions in the Ordinances for amending the State Budget Law.

As we previously mentioned, the institution had been obliged in this context to take the decision of postponing some investments.

ANNEX I

Decisions with normative character

Issued by the

Supervisory Authority

DECISION:

Regarding the recognition of an adequate personal data protection level in Jersey

By virtue of art. 3 paragraph (5) and (6) from the Law no. 102/2005 with regard to setting, organization and functioning of the National Supervisory Authority for Personal Data Processing, with the subsequent amendments and completions and of the art.6 paragraph (2) letter b) from Organization and functioning Regulation of the National Supervisory Authority for Personal Data Processing.

- issued in applying the provisions of the art. 29 paragraph (1) and (4) (2) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data, with the subsequent amendments and completions.

- in order to establish the implementation of the European Parliament and of the European Council Directive 95/46 with regard to the personal data processing and on the free movement of such data;

- for transposing the European Commission Decision no. 2008/393/EC, adopted based on the European Parliament and by the European Union Council Decision 94/46/EC with regard to the processing of personal data and on the free movement of such data, referring to the establishment of an adequate protection level of such personal data in *Jersey.*

- taking into consideration that *Jersey* is considered to be a third state according to the Directive 95/46/EC,

- taking in consideration the Law from 1987 with regard to the protection of personal data in Jersey, effective starting with 11th of November 1987 and of other complementary laws - The data protection Law from 2005 (Amendment) and the coming he Law from 2005 (Ammend5 (Amendment) and of the coming into force of the data protection law of 2005.

- taking into consideration that the ratification by Great Britain of the Convention from 28th of January 1981 for persons' protection against automatic personal data processing (European Council Convention no. 108) has also been extended to Jersey starting with 1987,

- seeing the Approval Paper no. 13 from November 18th, 2008 of the Authorization Bureau within the National Supervisory Authority for Personal Data Processing referred to the proposition of issuing a decision regarding the recognition of an adequate personal data processing level in *Jersey.*

The president of the National Supervisory Authority for Personal Data Processing presents the present decision:

Art. 1. The personal data transfer to *Jersey* can take place with respecting the provisions of the art. 29 paragraph (1) and paragraph (2) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data, with the subsequent amendments and completions, because in this state an adequate protection level of the personal data is ensured.

Art. 2 – (1) National Supervisory Authority for Personal Data Processing can dispose the interdiction or suspension of the personal data transfer to *Jersey,* in order to ensure the persons' fundamental rights with regard to personal data processing, in one of the following cases:

(a) a competent authority from *Jersey* has established that the personal data receiver has broken the applicable protection norms;

(b) exists the possibility of not respecting the personal data protection norms, in the conditions in which the Jersey competent authorities do not take adequate measures for protecting these data, making so that the transfer presents the risk of serious prejudice of the persons in question, and the receiver established in *Jersey* has been announced previously of adopting this measure in a reasonable term for providing an answer.

(2) Interdiction or suspension disposed according to the paragraph (1) will disappear, immediately after the National Supervisory Authority for Personal Data Processing has been announced that the reasons for taking these measures had stopped.

(3) The Romanian competent authorities will immediately inform the European Commission of the adopted measures according to the paragraph (1) and (2).

(4) The Romanian competent authorities and the European Commission will inform each other regarding the cases provided in the paragraph (1) when through the adopted measures by the *Jersey* responsible authorities, the personal data protection norms are not respected.

Art. 3 – The present decision transposes the European Commission Decision no. 2008/393/EC, adopted based on the European Parliament and by the European Union Council Decision 94/46/EC with regard to the processing of personal data and on the free movement of such data, referring to the establishment of an adequate protection level of such personal data in *Jersey,* published in the European Commission Official Journal no. L 138/21 from May 28, 2008.

Art. 4 - This Decision shall be published in the Romanian Official Gazette, Part I

The President of the National Supervisory Authority for Processing of Personal Data

Georgeta Basarabescu

No. 90 from November 26, 2008

DECISION:

For establishing the printed form of the notifications provided by the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data

Issued in applying the provisions of the art. 21 paragraph (3) letter a) reported at the art. 22 paragraph (3), (6) and (8) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data, according to which the supervisory authority has issued printed forms of the notifications, in the law provided situations:

- considering Romania's quality of member state with full rights of the European Union;

- having regard to the proposal from the European Commission expressed in the Report no. 1227/2005 of the Art 29 Working Group 29/2005 for data protection, regarding the importance for standardizing and simplifying the notification procedure of the national supervisory authorities, as well as adopting some less costly methods for putting them in practice in order to avoid the excessive administrative formalities;

- considering the provisions of the **European Parliament and by the European Union Council Decision 94/46/EC with regard to the processing of personal data and on the free movement of such data,** presenting that the notification is destined to ensure the purpose publicity and that of main characteristics of the personal data processing done by operators, so that the authority can control the concordance of the data processing declared with the national legal framework in the field;

- taking into consideration that, according to the law, mainly through the notification, the **information of the public upon the personal data processing declared by the operator through the personal data processing Register is ensured;**

- taking into consideration the fact that the notification tax has been repealed by the Government Emergency Ordinance no. 36/2007 for repealing the Law no. 476/2003 with regard to the notification tax repealing for the personal data processing, incident to the Law no. 677/2001

with regard to the personal data processing and on the free movement of such data, approved through the Law no. 278/2007 published in the Romanian Official Gazette, Part I 708 from November 19, 2008

- considering the situations in which the personal data processing notification based on the Decision no 90/2006 is not necessary, published into the Romanian Official Gazette, Part I, no. 650 from July 27, 2006, by the Decision no. 100/2007 regarding the situations in which the personal data processing notification is not necessary, published into the Romanian Official Gazette, Part I, no. 823 from December 3, 2007 as well as the personal data transfer notifications to other states, provided by the Decision no. 28/2007 with regard to the personal data transfer to other states, published in the Romanian Official Gazette, Part I 182 from November 16, 2007,

- seeing the Approval Paper no. 8 from June 5, 2008 with regarding to the necessity of modifying the notification printed forms, with the purpose of simplifying them,

By virtue of art.3 paragraph (5) and (6) from the Law no. 102/2005 with regard to setting, organization and functioning of the National Supervisory Authority For Personal Data Processing and of the art.6 paragraph (2) letter b) from Organization and functioning Regulation of the National Supervisory Authority for Personal Data Processing.

The president of the National Supervisory Authority For Personal Data Processing issues the present decision:

Art. 1

It is hereby approved the printed form of the notification provided by the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data, provided in the annex making part of the present decision.

Art. 2

Completing notifications on the approved forms, through the Decision no. 60/2006 for establishing printed forms of the notifications provided by the Law no 677/2001 for the personal data processing and on the free movement of such data, registered in the personal data evidence register up to the date of the present decision, they remain valid.

Art. 3 - This Decision shall be published in the Romanian Official Gazette, Part I and becomes effective starting March 1st,2009.

Art. 4 - On the date of entry into force of the present decision, Decision no. 60/2006 for establishing some printed forms of the notifications provided by the Law no 677/2001 for the personal data processing and on the free movement of such data, published in the Romanian Official Gazette, Part I, no. 506 from June 12, 2006, it ceases its application.

The President of the National Supervisory Authority for Personal Data Processing,

Georgeta Basarabescu

No. 95 from November 11, 2008

DECISION:

For the issuing procedure of the authorization for personal data processing regarding the health state, in the conditions of the art.9 paragraph (3) and (4) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data

Issued in applying the provisions of the art.21 paragraph (3) letter c) reported at the art.9 paragraph (3) and (4) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data, with the subsequent amendments and completions.

Seeing the Approval Paper no. 14 from November 18th, 2008 of the Authorization Bureau within the National Supervisory Authority for Personal Data Processing referred to the proposition of issuing a decision regarding the recognition of an adequate personal data processing level of the health state, in absence of the written and unequivocal consent of the person in question,

Taking into consideration the provisions of the European Parliament and European Council Directive 95/46/CE, with regard to the processing of personal data and on the free movement of such data, according to which the member states can derogate from the interdiction to process special data when this is justified by reasons of important public interest to some domains such a public health or health insurance.

Considering that in some circumstances the data subject is in the impossibility of given its consent or refuses to give it for the processing of his personal data, especially those regarding the health state.

Considering that the fundamental right to an intimate, family and private life can be limited with the purpose of realizing some public interest, as well as for protecting the public health or that of protecting life, physical integrity or health of other person than the data subject,

Seeing the exception under the art.7 paragraph (2) from the Law no. 677/2001 with the subsequent amendments and additions, according to which the data processing regarding the health state can be done when the law expressively provides, with the purpose of protecting an important public interest, with the condition that the processing is done with respecting the data subject rights and also of the other warranties provided by the Law no. 677/2001,

Seeing the warranties provided by the Law no. 677/2001 with the subsequent amendments and additions, according to which the data processing regarding the health state can be done only by or under the supervision of a medical person submitted to the professional secret, or by the other person submitted to an equivalent obligation regarding keeping the secret.

Taking into consideration the principles established by the art.4 from the Law no. 677/2001, with the subsequent amendments and completions, according to which the persona data must be processed in good faith and according to the effective legal provisions, collected for determined purposes, explicit and legitimate.

Considering the fact that the art.22 from the Law no. 677/2001, with the subsequent amendments and completions, imposes the operator the obligation to notify the National Supervisory Authority for Personal Data Processing before doing any processing or of any processing ensemble, having the same purposes

By virtue of art. 3 paragraph (5) and (6) from the Law no. 102/2005 with regard to setting, organization and functioning of the National Supervisory Authority For Personal Data Processing, with the subsequent amendments and completions, named hereinafter the National Supervisory Authority, as well as of the art. 6 paragraph (2) letter b) and art. (8) from Organization and functioning Regulation of the National Supervisory Authority For Personal Data Processing, approved through the Senate Permanent Bureau Decision no. 16/2005,

The president of the National Supervisory Authority For Personal Data Processing issues the present decision:

Art. 1 (1) Processing the personal data regarding the health state, with the purpose of protecting the life, physical integrity and health of other persons than the data subject or of the public in general, in the situations in which the data subject did not consent in writing and in an unequivocal way, can be done by the operator only after him obtaining the authorization of the National Supervisory Authority.

(2) The authorization model referred to in the paragraph (1) is established through the annex being integral part of the present decision

Art. 2 (1) In the authorization issuing process provided in the art. (1) the following conditions must be respected:

a) Notify the National Supervisory authority in the conditions of the art.22 from the Law no. 677/2001 with the subsequent amendments and completions, or where applicable by the completion/amending of a previously registered notification.

b) filling a solicitation together with the exculpatory documents containing at least the following information: the purpose of data processing, category or categories of the in question persons, personal data processed, estimated data for completing the processing

operation, collecting source of the personal data, description of the data processing conditions and, where applicable of the reasons justifying the emergency.

(2) If the solicitation provided in the paragraph (1) letter b) in incomplete, the National Supervisory Authority can solicit information and supplementary documents.

Art. 3 If the conditions established by the art 1 and 2 are not fulfilled, the National Supervisory Authority will instruct the solicitor in that direction.

Art. 4 (1) For issuing the authorization, the National Supervisory Authority solicits for the consultative notice of the Romanian College of Physicians.

(2) The provisions of the paragraph (1) are not applicable in case of the existence of justified emergency reasons , according to the art. 2.

Art. 5 This Decision shall be published in the Romanian Official Gazette, Part I and becomes effective starting February 1st2009.

The President of the National Supervisory Authority for Personal Data Processing,

Georgeta Basarabescu

No. 101 from December 29, 2008

ANNEX

AUTHORIZATION

No. ..... From:…

regarding the health state processing of personal data, in the conditions of the art. 9 paragraph (3) and (4) from the Law no. 677/2001 with regard to the personal data processing and on the free movement of such data

By virtue of art.21 paragraph (3) letter c) reported at the art. 9 paragraph (3) and (4) from the Law no. 677/2001, with the subsequent amendments and completions,

Taking into account:

Demand no. from:…

Presented by

Processing purpose:

.....

Category or categories of the persons in question:

.....

processed personal data:

.....

Estimation date for completing the processing operations:

.....

Data collecting source of personal data

.....

Data processing conditions:

……

Reasons justifying the emergency:

……

Solicit the consultative notice of the Romanian College of Physicians.[6]

[6] Except the emergency reasons.

The President of the National Supervisory Authority for Personal Data Processing,

AUTHORIZES

Processing of personal data regarding the health state, done by .....[7], processing notified with the no. .....[8].

Processing of the personal data outside the limits established by the authorization is forbidden.

The present authorization does not exonerate the operator from accomplishing the other obligations incumbent under the Law no. 677/2001, with the subsequent amendments and completions, including the obligation to be subjected to the control by the National Supervisory Authority.

According to the law, the National Supervisory Authority can dispose of any measure where it is established the breach of the operator's obligations.

PRESIDENT,

Georgeta Basarabescu

[7] Operator name/denomination
[8] Numărul de înregistrare a notificării din registrul de evidență a prelucrărilor de date cu caracter personal.

ANNEX 2

De lege ferenda suggestions

A) **Modification suggestion of the Law no 677/2001**

From the three years activity of its establishment and after applying the dispositions of the Law no. 677/2001, the Supervisory authority has been confronted in practice with more situations leading to the conclusion of the necessity to modify some articles of the previous mentioned law.

So, we consider that the art 2 paragraph (2) letter c) must be modified, considering Romania's quality of Member state with full rights of the European Union starting with January 1st, 2007. A clear distinction must be made between the operators' localization on the community's territory and those of the member states.

Art. 3 letters e), f), g) and h) defining the terms of "operator", "mandate", "third" and "receiver", needing a modification regarding the correction of the present definitions which should include also the non-juridical entities category, in accordance to the Directive 95/46/EC.

We propose including the definition of the notion "representative" in the Law no. 677/2001, in order to avoid the frequent confusion of the operators with the term used in the common law – that of legal representative.

To highlight the specific consent of the processing and protection of personal data in accordance with Directive 95/46/EC, is necessary to define it as "any manifestation of will, free, specific and informed, through which that person agrees that his personal data is to be processed".

To avoid possible excesses of the operators, such as to obstruct the right of access, due to the lack of regulation, is necessary to establish a maximum tax limit that operators can charge to exercise this right more than once during a year (when the law provides for free).

We suggest the modification of the art. 20 paragraph (5) regulating the data processing by authorized person *under a contract* concluded in written form by the operator and empowered, for the purposes of broadening the scope by replacing the term contract with that of *legal act,* in considering, for example, the quality of operator / empowered person of public law.

In addition, in the art.21 paragraph (3) is necessary to introduce a measure prohibiting the processing, which is found in other articles (for example, in the art 25 paragraph 5), as well as that of applying the contravention penalties.

Prohibition is a distinct termination measures because concerns the situation where the processing has not yet begun.

Setting a deadline of at least one year for filing the complaint to the Supervisory Authority, as is provided in the art. 25, a term necessary having regard to the legal terms that can be held liable operators violating Law no. 677/2001.

At the same time, we suggest that, in cases of an extreme complexity, the president should be able to decide the increase of the period the complaints are solved from 30 days to 60 days, in order to enable the Authority to carry out all the necessary demarches permitted by law, for a fair resolution of the referred aspects.

However, it is necessary that the persons concerned on behalf of which the Supervisory authority can act in court proceedings, to acquire an active part in a lawsuit (plaintiff), for the judgments' opposability.

Modification of the art.26 paragraph 1, by eliminating the term "irrevocable", so as to eliminate the only jurisdiction degree established in the present.

Amending the Chapter VII title governing the "transfer of personal data to third countries" is necessary to put in line with Directive 95/46/EC, and especially to give clarity of the text regarding the transfer to countries outside EU and EEA, in view of Romania's quality of EU Member State.

Also about the transfers of data, it is necessary to unitary specify the situations where, although the receiving State does not ensure an adequate level of protection, the data transfer may be allowed in third countries, including the situation in which the guarantees are provided by other instruments than contractual clauses, such as compulsory internal rules corresponding to those recognized at European Union level *(Binding Corporate Rules).*

B) **Modification suggestion of the Law no 9 paragraph (3) from the Law no. 506/2004 on the processing of personal data and intimate life privacy in the electronic communications sector, with subsequent amendments and completions**

The National Supervisory Authority considers the modification of art 9 9 paragraph (3) from the Law no. 506/2004 to be necessary, so as to establish by law, the resolution conditions of complaints regarding abusive calls, in a manner similar to that existing in most Member States of the European Union.

In this regard, regulations having an incidence in this area are stated by acts at law or issued by the government, and the jurisdiction solution is that of the national communication authorities.

C) Modification suggestion of the Law no 23 paragraph (1) from the Law no. 365/2002, of the electronic commerce, with the subsequent amendments and completions

Art. 23 paragraph (1) from the Law no. 365/2002 establishes an alternative power between the National Supervisory Authorities and the National Authority for Communications, on finding the contravention referred to in art. 22 letter a) of the same legislation and application of the appropriate penalty.

Regarding the unsolicited commercial communications, the Supervisory authority has already established functions in the field of electronic communications, respectively by Law no. 506/2004 concerning the processing of personal data and privacy in the electronic communications sector, according to which it defends the individuals' rights of sending them electronic messages only with their consent.

Therefore, in order to eliminate contradictions and parallels of the effective legislation, in conjunction with the Supervisory authority powers established by Law no. 506/2004, we suggest the modification of the art. 23 paragraph (1) from the Law no. 365/2002 for the purposes of only maintaining the power to control of the National Authority for Communications

D) Suggestion regarding the elimination or modification of the art 20 from the Law no. 298/2008 dispositions, regarding the retention of data generated or processed by providers of electronic communications services to the public or public communications network and for the Law no. 506/2004 amendment, law concerning the processing of personal data and privacy in the electronic communications sector

Through the Law no. 298/2008 it is aimed at regulating the national obligation level of service providers and public network of electronic communications to retain certain data generated or processed in their provision of electronic communications services, as well as for putting them to the competent authorities' disposal, for their use in the framework of research, discovery and prosecution of **serious crimes**.

We mention that disclosure of the data retained by providers of public communications network and service providers of electronic communications is done on the basis of authorization issued by the judge or, in emergency cases, by the prosecutor performing of supervising the prosecution.

Plus, we mention that in case of notice, the art. 20 of the Law no 288/2008 project did not include the provisions governing the access mode of the responsible state organs for defending the national security. By the ambiguous wording mode of this article different interpretations of laws can appear, and the created situations might affect the privacy of individuals.