CENTRUL NAŢIONAL PENTRU PROTECŢIA DATELOR CU CARACTER PERSONAL AL REPUBLICII MOLDOVA

MD-2004, mun. Chişinău, str. Serghei Lazo, 48, tel: (+373-22) 820801, 811807, fax: 820807, www.datepersonale.md

ORDER no. _____

„__" May 2013 **Chişinău mun.**

On approval of Instructions on the processing of personal data in the police sector

Pursuant to Art. 20 para. (1) letter c) of Law No. 133 of 8 July 2011 on personal data protection, Chapter II, Art. 3 letter. e^2) of the National Center for Personal Data Protection Regulation, structure, staff - limit and its financial arrangements, approved by Law No. 182-XVI of 10 July 2008

I ORDER:

1. To approve the Instructions on the processing of personal data in the police sector (attached).

2. It is recommended for consideration of the Office of the Prosecutor General the Instructions within adapting personal data processing procedures by the authorities engaged in the police sector, to the principles stated by the legislation governing personal data protection.

3. Legal and Public Relations Department, together with Evidence and Control Department will ensure the placement of Instructions on the processing of personal data in the police sector on the official website of the National Center for Personal Data Protection of the Republic of Moldova (www.datepersonale.md).

Vitalie PANIŞ
Director

Unofficial translation

INSTRUCTIONS
on the processing of personal data in the police sector

Preamble

The National Center for Personal Data Protection of the Republic of Moldova (the Center), aware of the progress of information technology and the move to automated methods of personal data processing ;

in order to prevent unauthorized processing of personal data stored in automated filing systems in terms of consultation , retrieval and their use excessively for declared goals ;

taking into account security incidents detected by the Center, such as: the annexation to materials of contraventional or criminal cases of personal records retrieved from the State Register of Population or copies of ID cards and their annexes on which are recorded personal data that are not required for these processes *(personal data aimed at children , eye colour, blood type, height, information on marital status , information about participation in elections , nationality , etc.*); not respecting the confidentiality and security of personal data processing by unauthorized disclosure of the contents of calls' intercepts made under prosecution procedure; unauthorized access to the security perimeter of the prosecution bodies which makes possible subsequent unauthorized access to personal data; consultation of information stored in main state information resources in the absence of legal grounds for making such transactions etc.,

taking into account that :

- the exchange of personal data in the framework of police bodies cooperation , in accordance with the availability of information principle, should be supported by clear rules , that enhance mutual trust between competent authorities, to ensure the protection of relevant information and respect of the fundamental rights of individuals ;
- it is necessary to specify the objectives of personal data protection in the framework of police activities and set rules that would ensure that any information collected is processed lawfully and in accordance with the fundamental principles of data quality ;
- any action of disclosure of personal data, including those that are not related to criminal, contraventional activities and, where appropriate, civil activity, must respect the fundamental rights and freedoms of the persons concerned , including the right to protection of personal data ;

taking into account the importance and role of prosecutors in the criminal justice system, including the fact that the quality of prosecutors activities directly reflects the level of democracy in a state of law and ensuring a fair process and orderly functioning of the criminal justice system can only be achieved when all relevant stakeholders will perform their tasks correctly, consistently and rapidly, respecting and protecting human dignity and human rights;

considering that the Office of the Prosecutor General has the role of guarantor in respect of the implementation of the binding nature of criminal procedural law by controlling compliance of procedural actions with the provisions of the Code of Criminal Procedure, other normative acts, as well as international acts, including by way of issuing methodological and regulatory guidelines related to law enforcement issues and the efficiency of combating and preventing crime, -

has developed these Instructions on the processing of personal data in the police sector .

I. GENERAL PROVISIONS

1. The Instructions on the processing of personal data in the police sector (Instructions) were developed without touching the jurisdiction of the Office of the Prosecutor General , taking into account the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms; the Convention on the protection of individuals with regard to automated processing of

personal data; Havana Rules, adopted by the Eighth United Nations Congress on the prevention of crime and treatment of offenders, Recommendation 1604 (2003) of the Parliamentary Assembly of the Council of Europe on the role of the public prosecutor's office in a democratic society governed by the rule of law; Code of Criminal Procedure of the Republic of Moldova; Contravention Code of the Republic of Moldova; the Law on personal data protection; the Law on Prosecution ; Requirements for the assurance of personal data security at their processing within the information systems of personal data approved by Government Decision no . 1123 of 14 December 2010; Regulation to the Register of evidence of the personal data controllers, approved by Government Decision no. 296 of 15 May 2012; the Regulation of the Office of the Prosecutor General, approved by Prosecutor General Order no. 52/3 of 21 June 2010; the Code of Ethics of the prosecutor, approved by Decision of the Superior Council of Prosecutors no. 12-3d228/11 on 04 October 2011.

2. The Instructions can serve as guidelines in order to bring the processing operations of personal data carried out by prosecutors and entities involved in policing in accordance with the principles enshrined in the Convention on the Protection of Individuals with regard to Automated Processing of Personal Data, Law on personal data protection and best practices.

3. Terms used in the text:

personal data - any information relating to an identified or identifiable natural person ('personal data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. **For example:** name, surname, year of birth, residence, state identification number (IDNO), photos and video - represent personal data relating to a directly identified individual. In the process of prosecution, the individual may be collected some other personal data such as signature applied to the preparation of papers / projects, fingerprints, etc. However, the statements made by participants in the process and recorded in the minutes of the hearing, also represent personal data related to individuals interviewed or identified or identifiable third persons involved in the commission of a harmful act.

special categories of personal data – data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, social belonging, data concerning health or sex life, as well as data relating to criminal convictions, administrative sanctions or coercive procedural measures. **For example,** information contained in: medical certificates / forensic reports, criminal record, Annex to the ID (*stamps "Referendum 2010" election", because in certain circumstances may swiftly reflect certain political beliefs*), etc. At the same time, information about people in hospitals, nursing homes for the elderly or held on an arrest until the sentencing of the court, relating to persons sentenced to prison, those serving a sanction of arrest, in prisons institutions represent special categories of personal data.

processing of personal data – any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, keeping, restoring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

controller – a natural or legal person governed by public law, or by private law, including public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data expressly provided by applicable law. **For example,** in all cases where the Office of the Prosecutor General shall regulate by a normative departmental act the goals and procedures for collection, storage and further processing of certain personal data in the automated filing systems, manual or mixed, it will be stated as the controller of such data.

processor – a natural or legal person governed by public law, or by private law, including public authority and its territorial subdivisions, which processes personal data on behalf of the controller, on instructions from the controller. **For example,** territorial / specialised prosecutions are processors when they process personal data in accordance with Instructions approved by the Office of the Prosecutor General.

filing system of personal data - any structured set of personal data accessible according to specific criteria, whether centralized, decentralized or distributed according to functional or geographical criteria. As filing system of personal data consists including but not limited to, databases, information systems where are stored and processed automatically or manually personal data. **For example**, classical models of filing systems of personal data are: Register of evidence of the Prosecutor's employees or corporate telephone numbers of employees of the Prosecutor, Register of Visitors, Register of petitions and other addressing, personalized information about specialized training of prosecutor's employees or other subjects involved in the instructional process, etc. other structured set of personal data, such as video images collected by a video surveillance system installed inside or on the perimeter of the prosecutor's office and etc.

depersonalisation of data – is such alteration of personal data so that details of personal or material circumstances can no longer be linked to an identified or identifiable natural person;

police activity - all actions / inactions taken by law enforcement authorities (*police*) to prevent / combat / investigate harmful events (*crimes and offenses*) and maintain public order.

II. ORGANIZATIONAL AND TECHNICAL PROCEDURES THAT MUST BE FOLLOWED

4. It is recommended that entities involved in the criminal or contraventional activity to be allotted, depending on the role they have, the quality of controller or processor, in accordance with the terms stated by the Art.3 of the Law on personal data protection and point 3 of these Instructions. This will allow clear separation of powers and the appropriate allocation of rights and obligations within the processing operations of personal data.

5. All persons involved in activities stated in point 4, who process personal data, including employees of the prosecution, will be subject to a confidentiality statement, which, as appropriate, may be included in contracts of employment, as having contractual clause, or within the job descriptions, mentioning about civil, criminal or contravention liability for its breach.

6. It is to be developed and implemented the security policy of personal data in accordance with the provisions of the Requirements for the assurance of personal data security at their processing within the information systems of personal data approved by Government Decision no. 1123 of 14 December 2010 (Requirements), which would cover issues referring to: procedures and measures related to security policy making, applying practical solutions with a wide related details and proportionate complexity level; identifying and authenticating users with access rights to the information systems of personal data; reactionary ways to security incidents; protection of information technology and communications; ensuring information integrity that contain personal data; management of access to personal data processed; audit in information systems and filling systems of personal data, etc.

7. Security policy is to contain provisions that ensure the protection of personal data processed within filling systems held, in particular through the following methods:
- prevention of unauthorized connections to communications networks and interception by technical means of personal data transmitted via these networks, especially while disclosure by transmission of personal data between different entities vested with powers in activities related to the processing of

personal data within the framework of prevention and investigation of crime, enforcement of judgments and other actions of criminal or contraventional proceedings;
- exclusion of the unauthorized access to personal data processed within filling systems by means of implementing procedures for identification and authentication of users; by distribution of duties and investment with the minimum rights and competencies of those involved in the management of filing systems of personal data; by ensuring the integrity of information resources (*data and programs*);
- prevention of specific technical and program actions which makes destruction, modification of personal data or failure in technical and programming complex work, of software for processing personal data by means of special technical and program protection methods, also using licensed programs, antivirus programs, organizing control system of software security and performing regular backups;
- prevention of intented and/or unintended actions of local and/or external users, and other employees conditioning the destruction, modification of personal data processed in filling systems or failures in technical and program work;
- prevention of leakage of information containing personal data, transmitted via connecting channels, using encryption methods (*encryption*) of such information;
- precise establishment of order and procedures of access to information containing personal data processed within information and filling systems, both for local and external users;
- organizing generating of audit records of security in information and filling systems of personal data for making possible the accumulation of evidences in cases investigating possible access operations / attempted unauthorized access, modification operations, extraction, blocking, erasure or destruction of personal data processed in these filling systems.

8. When happens the disclosure of the electronic format of personal data contained in the criminal, contraventional and/or civil records, in accounting records containing personal data of the employees and other documents related to the employees, via communication networks or on other digital storage, it will be ensured the encryption of this information or it will be examined the possibility of using a bilateral connections via VPN secure channel. Wireless access to the filling systems of personal data is to be allowed and authorized only if using cryptographic means for protection of information. Each case of requirement for transmission of personal data electronically will be considered separately, given the technical possibilities of the recipient and controller, as well as in accordance with organizational and technical measures implemented by the parties. In case if the communication networks pose a risk to confidentiality and security of personal data, there will be used traditional methods of transmission (*mailing with recommended notice, personal handing, etc.*).

9. Disclosure by transmission of personal data through communication networks that do not meet the Requirements, (*e.g.: sending information via personal e-mail such as @gmail.com, @ mail.ru, @ yahoo.com, etc*.) will be prohibited.

10. It is to be prohibited to disclose personal data between prosecutors or authorities exercising police activities in the Republic of Moldova to entities geographically located on the left bank of Dniester river and refuse to obey the legislation of the Republic of Moldova, based on the consideration that at the moment it is not possible to exercise effective control over this part of the territory, including in respect of personal data processing compliance with the Law on personal data protection. **For example**: on 04 January 2013, after examining the complaint of a group of people, the Center issued the decision of suspending the processing of any personal data, through which the Ministry of Internal Affairs was asked to suspend any operations of disclosure to the unconstitutional authorities from the administrative districts located on the left bank of Dniester, of personal data processed as controller or recipient, prior to the registration required by these entities in accordance with art.23 and 34 par.(4) of the Law on Personal Data Protection and the implementation of Requirements for the assurance of personal data security at their processing within the information systems of personal data, approved by

Government Decision no.1123 of 14 December 2010. Subsequently, this decision served as the basis for the Central Court to issue a decision by which the Court noted the breach of personal life privacy and personal data protection legislation by transferring personal data to the authorities and entities of the left bank of Dniester, which act outside of the field of national law, forcing the Ministry of Internal Affairs to compensate moral and material damages of over MDL 180,000. Moreover, by the Decision of the Superior Council of Magistracy of 10 April 2012 on the request of the Minister of Justice, on the opinion regarding the addressing of the Deputy Prime Minister on the approach of certain legal issues, it was stated that: *"... any act issued by the self-proclaimed authorities in this part of the Republic of Moldova, are contrary to the Constitution, in the first place, this fact refers to any decisions, order, decrees of courts established illegally in this region. Thus, the Council will consider as unacceptable any collaboration and co-working related to legal aspects and proposed judicial solutions with structures from the transnistrian region".*

11. Disclosure procedure by transmitting personal data stored on paper, including the cases of investigations conducted outside the Republic of Moldova, shall be regulated by institutional regulatory documents, taking into account the need to ensure an adequate level of personal data protection, including the usage of diplomatic channels. Personal data transfers across borders must be carried out in strict compliance with art.32 of the Law on Personal Data Protection, especially in cases where an international treaty, under which the transfer takes place, does not protect the rights of the personal data subject.

12. Volume and category of personal data collected in the context of crime prevention and investigation, prevention and investigation of criminal offences, enforcement of convictions and other activities within criminal or contravention procedures, needs to be limited to the minimum necessary to achieve the stated goals.

13. The Office of the Prosecutor General (*as appropriate, territorial/specialized prosecution*), will regulate explicitly, according to art. 15 and 212 of the Criminal Procedure Code, the procedure for access to the case file and witnesses, suspects, accused, victims, injured party, civil and civilly liable, defenders or persons empowered are to avoid the unauthorized disclosure of personal data, including the prohibition of taking unauthorized photos and videos in the security perimeter of Prosecutor's Office such as the usage of hidden technical means, taking into account the need to ensure the confidentiality and security of personal data processing, provided by art.29 and 30 of the Law on Personal Data Protection, and by section 26 of the Requirements. **For example**: actions such as video recording, in the process of examining criminal file no. 2010038002 and control material no.18 pr/13, with further posting of videos in the internet at http://www.youtube.com/watch?v=QnFGqTumx8Q and http://curajtv.play.md/ are to be excluded *per se*.

14. If the lawyer or an authorized person requests to examine the case materials, they will be informed in written form of their obligations in accordance with art.15 of Criminal Procedure Code, art.29 and 30 of the Law on Personal Data Protection, including on liability provided by art.74^1 of the Contravention Code and/or art.315 of Criminal Code.

15. Prosecutor's Office and other entities practicing activities in the police sector will review the terms of contract with the State Enterprise Centre for State Information Resources "Registru" in order to fully cover the provisions stipulated in art.4 par.(1) points a) b) c) d) and e) of the Law on Personal Data Protection. In this regard, authorized persons shall have access only to those categories and amount of personal data stored in the main state information resources which are directly related to the purpose for which it is accessed or collected. Thus, the individualized access to each category will exclude the possibility of processing an excessive volume of data aimed at subjects or purposes other than originally intended. **For example**: it was found that in 80 % of cases Criminal Prosecution officers or prosecutors consult the State Population Register to identify the place of residence of witnesses and other participants in the process order to to summon to attend hearings. In this case the data which are presently available (*name of children, parents, spouses, blood type, height, eye color, properties etc*.) are not necessary for the purpose originally intended.

16. Prosecutors, before initiating the authorization procedures by the coroners of special investigative measures, are to assess the proportionality of the interference in the private life of a person admitted as per intended purpose, and are to decide, on their own responsibility, if the restriction of rights and freedoms of individuals, particularly the right to privacy is necessary. In the process of decision making regarding the initiation of the authorizing process in order to carry out special investigative activities, the representatives of the competent authority shall take into account the provisions of art.4 (1) of the Law on the Personal Data Protection which states that personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed. This very principle of personal data protection, in conjunction with art.15 and 132^1 paragraph (3) of the Criminal Procedure Code is to be applied upon deciding to apply special investigative measures. **For example**: the relevant situation frequently detected by the Center through mobile operators, in a criminal case on the theft of a mobile phone, they are requested to disclose personal data aimed at subscribers who used or were called by this phone using the IMEI number, information which can be recorded on dozens or even hundreds of pages, when in fact the information that will be used in court is the one regarding subscribers that have/been called most often, usually a few people, who might help identify the suspect after hearings. In these situations, the amount of processed personal data is excessive, and interference with the privacy of individuals in relation to the stated purpose is, apparently, unjustified.

17. Personal data stored in the State Register of the population and other main information resources of the state, are to be consulted only if the action is motivated and justified in terms of legal and personal records retrieval from the automated system/s, is to be done only in exceptional cases, following that the extracted statement is not stored for a period exceeding the intended purpose. Further on, after achieving the purpose for which they were extracted, personal records are to be destroyed following a decision in this regard. In the same train of thoughts, the privacy and security of personal data recorded in the extracted personal files should be distinctly regulated. It follows that during the time necessary to conduct preliminary inquiry these are kept separately in another file and will not be attached to the criminal file and will not be made known to the parties, except the concerned person. It will be explained that extracting personal files of non-participants to the criminal process in order to use photos included in these documents to achieve procedural action under art.111 par. (6) of the Criminal Procedure Code-submitted for recognition, is unacceptable and breaches the principles of art.4 par.(1) point b) of the Law on Personal Data Protection, including the provisions of art.74^1 par.(4) of the Contravention Code.

18. Are to be revised categories of personal data which are collected and included in the trial documents prepared by prosecutors or by criminal prosecution officers, so that these are not excessive in relation to provisions of art.15 of the Criminal Procedure Code. **For example:** in the hearing proceedings of the witnesses, one will indicate only their names and addresses, based on art.105 of the Criminal Procedure Code. Simultaneously, the proceedings will be prepared in compliance with art.260 of the Criminal Procedure Code, which expressly stipulates the elements to be included in the report. Thus, the collection of personal data categories that are not in the article cited above will be prohibited or motivated in written form in the report, in accordance with art. 15 par.(3) of the Criminal Procedure Code.

19. Actions must be taken to exclude cases of use by prosecutors or representatives of authorities exercising activities in the police sector, of the situation of public service and resources to check whether they are or not monitored by other law enforcement bodies. **For example:** the Center found several cases where mid-level decision makers, requested from the State Enterprise CSIR "Registru" information from the audit of information systems on entities and authorized users who have consulted and extracted personal records of subordinate police officers, including prosecutors. The purpose for requesting this information in one case– "the need arising from criminal prosecution in a case initiated under art.284 of the Criminal Code (*organizing and running a criminal organization*)" was not a real one. The reason behind this was the desire to know whether the information on prosecutor and employees of the Ministry of Internal Affairs who were investigating this crime was consulted by other

entities in order to avoid the possible danger of disclosure to suspicious people. In this case, however, the information could only be requested by the Prosecutor General in criminal proceedings, which would specifically indicate any preparation facts or attempts to commit a crime against the prosecutor conducting criminal prosecution or police officers involved in the investigation and criminal prosecution of the offense under art.284 of the Criminal Code.

20. It will be explained that in accordance with art. 157 of the Criminal Procedure Code, any form of documents (*written, audio, video, electronics, etc*.) originating from official physical or legal persons which expose them or authenticated circumstances that matter for the cause (*including data stored in information and filling systems*) can be requested through a process of criminal prosecution body or the criminal trial process. In this case, however, the provisions of art.214 of the Criminal Procedure Code shall be observed, which provide that during criminal proceedings official information with limited accessibility cannot be unnecessarily administered, used or disseminated. Persons to whom the criminal prosecution body or the court requires to disclose or provide official information with limited access (*including personal data controllers*) are entitled to be assured that these data are collected for the respective criminal proceedings and otherwise can refuse to communicate or present data. Persons to whom the criminal prosecution body or the court requires them to disclose or provide official information with limited access previously are entitled to receive in advance a written explanation from the person requesting the information, which confirms the need to provide mentioned data.

21. It must be kept in mind that in accordance with stipulations of art. 8 of the Law on access to information, personal data are part of official information with limited access, access to which is made in accordance with data protection legislation.

22. Certain personal data processed in information and filling systems (*digital fingerprints, handwritten signature, etc.*) can be collected and used in a criminal or contraventional process as samples required for comparative research only complying with art.157-156, 260-261 of the Criminal Procedure Code and art.4 of the Law on Personal Data Protection, by issuing motivated ordinances and elaborating appropriate proceedings. **For example**: the Center found in specific cases that the requesting actions through a simple demarche of criminal prosecution body, of digital fingerprints collected by the State Enterprise CSIR "Register" during the issuance of biometric passports contradict the principles of criminal procedure and personal data protection.

III. Rights of personal data subjects

23. When personal data are collected directly from the data subject, in accordance with art.15 of the Criminal Procedure Code and art.12 of the Law on Personal Data Protection, the requesting person shall be provided with the following information, except where he/she already has that information on:

- the identity of the controller or, where applicable, the processor (*name, legal address, IDNO, registration number in the Register of evidence of the personal data controllers*);
- the actual purpose of processing of the collected data;
- the recipients or categories of recipients of personal data, the existence of rights to information and access to the data collected; the intervention over the data (*especially to correct, update, block or delete personal data whose processing is against the law because of the incomplete or inaccurate nature of thereof*) and the opposition, as well as the conditions under which these rights can be exercised; if the answers to the questions with the help of which data are collected are obligatory or voluntary, including the possible consequences of refusing to answer the questions via which the information is collected.

24. Subjects of personal data will be guaranteed the right of access and opportunity to learn about the documents in order to verify the correctness of their establishment, appealing against their non-inclusion in or exclusion from the list, as well as against other mistakes done during the enrollment of his/her personal data. In this regard, the persons responsible for processing personal data will ensure the subject's access only to the personal data that concerns him/her directly, being excluded from the possibility of consultation of personal data that concerns other subjects, contained in the process documents (*materials of the cause*), except where the applicants have an legal interest that is not

prejudicial to the interests or fundamental rights and freedoms of data subject or cases stipulated by art.293 par.(1)of Criminal Procedure Code.

25. Right to information will be provided by the personal data controllers (*prosecutors or authorities exercising activities in the police*) to all persons subjected to special investigative measures specified in art.132^2 par.(1) point b), c) e), g) and n) of the Criminal Procedure Code, collateral inclusively, unless the informing concerned persons proves impossible or it involves disproportionate effort. Currently, despite the gravity of the interference, the people who contact the subject of special investigation measures and who can also be considered as a personal data subject collected and processed without his/her consent by the entities that perform special investigative activity - are not informed about it. Thus, the person is deprived of the possibility of achieving his/her rights as a personal data subject. **For example**: if the home of the suspect of committing acts prejudicial is subjected to measures of special investigation - surveillance and audio-video recording, subjects were contacted/communicated via telephone network or entered the residence of the person nominated, will be told as per terms and conditions of art.132^5 of the Criminal Procedure Code. Relevant in this respect are some statements of the European Court of Human Rights in *Amann vs Switzerland case*, which proved that one must regulate in detail the "fortuitous" supervised persons as "necessary participant" in a phone conversation recorded by the authorities on the basis of respective legal provisions.

26. When posting personal data processed in the internal filing systems through the official website of the Prosecution or the criminal prosecution bodies, is to be established the necessary technical solutions to exclude unrestricted access to it, being provided technical programming measures, specializing in information security, protective measures for unambiguous confirmation of the identity of personal data subject, who exercise their right of access and rectification, by exclusion of the unauthorized access to data. **For example**: in the case of the section entitled "interpellations and questions of the deputies" on the official website of the Office of the Prosecutor General Http://www.procuratura.md/md/ID/ , it was established as an important tool to inform the public and ensure decisional transparency in prosecutorial activity. Nevertheless, during the first period when the named section operated, information was disclosed without being depersonalized violating the principles of personal data protection, prompting the intervention of the Center.

27. When exercising by the personal data subject the right to intervention, the inaccurate data are to be updated by amendment or deletion, as base for using only legal sources (*identification documents, marital status documents, main state information resources etc*.) the amendment is to be done in all managed filing systems.

28. Disclosure by transmission, dissemination or otherwise of the personal data processed in legal purposes will be prohibited, except where personal data subject has given his/her consent, when the information is depersonalized or when the law or international treaty expressly stipulates the right of the recipient or of the third party to do so. In this case, the special law or the international treaty must guarantee protection to personal data subject.

29. Application of exceptions and limitations to achieving by personal data subjects of their rights is to be made in strict accordance with art.15 of the Law on Personal Data Protection and the 132^5 of the Criminal Procedure Code.

IV. Storage, retention and destruction of personal data processed in the police activity

30. Storage and retention of personal data registered in the procedural documents and control materials, is to be carried out in strict accordance with the art. 211-214 of the Criminal Procedure Code and to the Office of the Prosecutor General, the territorial/specialized Prosecutions, and criminal prosecution bodies will assume the right to decide on their finality taking into consideration the provisions of art.4 par. (1) point e) of the Law on Personal Data Protection.

31. The access to areas where are located information and filling systems of personal data are to be restricted, allowing only to those who have the necessary authorization and only during working hours, according to institutional security policy approved.
32. The storage and keeping of the electronic format of personal data, structured in filing systems that are connected to the Internet, are not equipped with special means of technical and program protection and do not have installed licensed programs, antivirus programs, systems of software security control, insurance for regular back-ups and audit performance – is to be prohibited.
33. Introduction to institutional security zone and use of personal computers or USB for service purposes is to be prohibited. **For example**: when the employees resign and the accumulated information was stored on the device's internal magnetic carrier, their personal computer will contain structured set of personal data collected in the process of activities related to criminal proceedings, administrative or other type, and in case of failure the person that will repair these machines can effortlessly copy the information stored in the computer, both situations being considered as serious security incidents. In this context, application of the principles concerning personal data protection needs to be regulated by orders and instructions from superiors, with periodic check of premises and equipment necessary for employees. Furthermore, access to computers equipment is to be protected / restricted by creating user profiles and administrator rights are to be entrusted only to the person responsible for implementing the security policy of the designated institution.
34. Storage of personal data on magnetic, optical, laser, paper or on other means of information on which is created, set, transmitted, received, maintained or otherwise it is being used the document which allows its reproduction, shall be ensured by placing them in safes or lockable metal cabinets and to seal them. Access to safes and metal cabinets is to be monitored by keeping an evidence register. Storage without authorization, of personal data bearers from the security perimeter of the controller is to be prohibited.