Study on personal data protection acts and regulations

Project Deliverable
D.1.1. Data collection and Planning

Alberto Leone_AlmaLaurea

Introduction

The standard architecture of the AlmaLaurea system, which has been entirely or partially reproduced in the various international projects, is such that the Universities involved in the project must periodically transfer administrative data concerning their graduates.

The data must be transferred in compliance with the personal data protection regulations that are in force in the country involved in the project and in Italy.

The aim of this document is to specify what kind of information is transferred and how it is processed, in such a way to obtain – if necessary – prior authorization from the government bodies (Data Protection Authorities, agencies, etc.) that are competent in this specific field.

System Overview

The system consists of a database of curriculum vitae created and managed by the graduates. Each CV is formed by merging information provided by the graduates and other information provided by the Universities (graduate data). The database is used by registered companies. Companies can search and download CVs only for placement purposes. No other use is allowed for downloaded data.
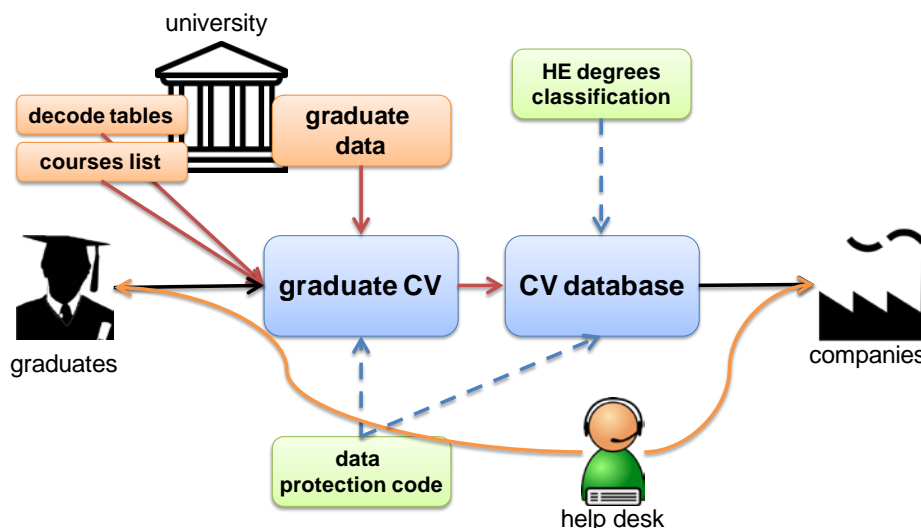
Merging data

The following figure represents data transmitted by universities and filled-in by the graduates (HEN-GEAR) Each row represents a student/graduate. Each column represents a particular item of information (e.g. name, last name, email, degree, final mark, English language skill, etc.).

As shown in the figure, if the University transmits all the data of its graduates there are three possibilities:
- Not registered. These data cannot be accessed by anyone. Only the technical management is allowed to access them (backup).
- Registered and certified. This record can be read by companies and managed by the HEN-GEAR staff. Some information about the degree is certified.
- Registered but not certified. Also this record can be read by companies and managed by the HEN-GEAR staff. Degree information is not certified.

when conflicting certified data has priority

university

student A (not registered)

student B
(registered and certified)

student C
(registered but not certified)

degree
internal code

final mark

foreign
language skill
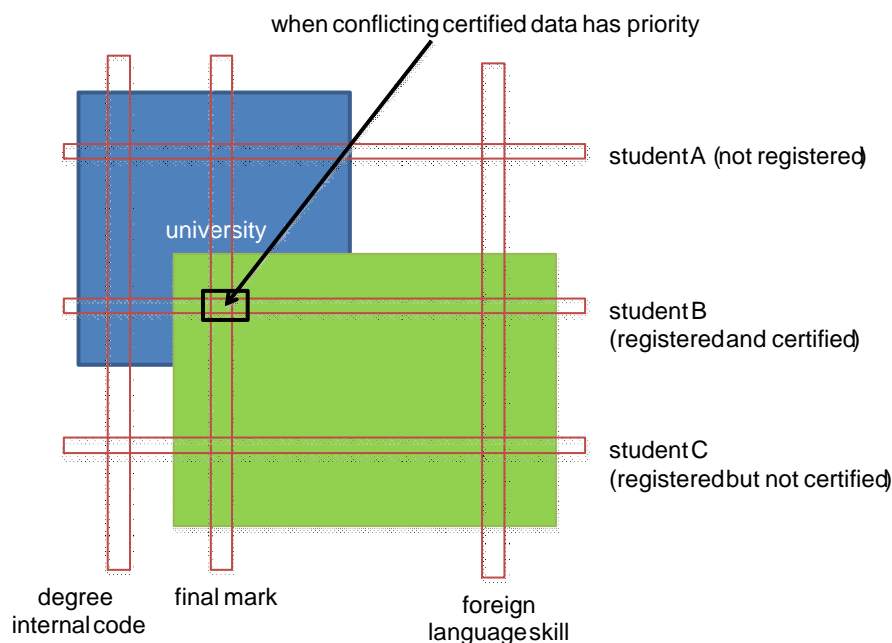
Data flow and processing

There are two possible *technological solutions* to manage the certification of graduates' data.

The *first one* is more substantial in terms of data processing, because it requires the transfer of all the data, also of those who do not participate in the project. This possibility must be provided for in the legal framework. It must also be specified if any authorization must be obtained, of which kind and how.

The *second solution* is less critical and it can be taken into consideration in the countries where the first solution cannot be applied. The advantage of the second solution is that, if necessary, there is the possibility of getting an authorization from the data subject at the time s/he registers on the system.

Solution 1. Massive transfer of the data of all graduates

- The graduates/students register on the system, create and manage their CVs. The data are stored on servers located in Italy
- The Universities transfer the data on the curricula of all the graduates of a given academic year
- These data are transferred in Italy and stored on the HEN-GEAR servers
- The AlmaLaurea staff selects through automatic procedures the graduates' data available in the database and transfers them in the DB
- The unused data remain stored in a separate database which is not accessible to companies and which is only processed for maintenance needs (backup)

Solution 2. Massive transfer of the anonymized data of all graduates + data for certification

This is a combination of the first two solutions. For the sake of simplicity, the data are transferred in parallel to pursue two different objectives:

1. **Data collection for statistical purposes.** The data of ALL the graduates are transferred once a year in an anonymous form, with a non-reversible personal identifier (only the university can trace the identity of the owner of each record)
2. **Certification**. Solution 2 is applied only to those registered in the database

Point (1) should not be subject to any legal constraint, given that the data are processed only in an anonymous form.

Types of processing

Integration of CVs

For the graduates who have registered on the system and have authorized their CVs to be processed, the administrative data are used to correct and certify the information provided by the graduates about the degrees they have achieved.

Statistical processing

The data are first integrated with the information collected through the questionnaires filled out by students who are about to graduate and then made anonymous. These data are used by researchers to carry out the statistical analyses that are part of the project. The results are only disseminated in an aggregate form, with all due measures being taken to make it impossible to identify individuals (for instance, no information is provided for groups of less than 5 people).
The administrative data are not processed in any other way.

Technical Activities

Technical activities necessary to manage the database (backup, database management)

Transferred information

Personal data. Personal identification data: first name, last name, date and place of birth, national identification numbers (e.g. CIN)
Contacts. Addresses, phone numbers and other contacts (email)
Information on degree: title of the degree, final mark, other information on the degree (title of the dissertation, enrolment date, date of graduation, etc.)
Information on prerequisite degree (if applicable): for second/third-level degrees, some information on prerequisite degree
Information on high school

The appendix contains the details of all the information that is transferred in each section.

Legal framework in the various countries

Legal references

The following table summarizes the situation in the various countries

Country	Personal data protection law	Government body
Italy	Codice in materia di protezione dei dati personali. DL 196/2003	Autorità garante della Privacy
Armenia	RoA Legislation on Personal Data Protection RA Law-422 (adopted October 8,2002)	Republic of Armenia

Notice/consent forms

Depending on the required type of processing, on the contents of data and on their geographical location, it may be necessary to provide a notice of privacy policy to the data subject, to have it signed as acknowledgement of receipt or to ask for explicit consent. Consent may be given in electronic form, or it may even be necessary to give it in written form (or through digital signature). This table summarizes the various scenarios.

Form	Description
None	The data subject does not have to receive any document. It is not required by law
Info	The data subject must receive a notice of privacy policy
Info-signed	The data subject must receive a notice of privacy policy and accept it through electronic signature
Consensus-light	The data subject must receive a notice of privacy policy and give explicit consent to one or more types of processing. Consent may be given in a "weak" form (electronic signature)
Consensus-hard	As above, but consent must be given through handwritten or digital signature

Compatibility matrix

Examples

The following table shows some (theoretical) examples. Country 1 has light regulations. Data can be managed according to Solution 1 and no action is necessary.

Country 2 allows for data transfer, but the University has to adapt its regulation by explicitly mentioning that a third party is authorized to manage some data with clear limitations and only to reach a specific goal (statistical analyses, simplify management for the implementation of a CV database).

The third example represents a Country where solution 1 is not allowed at all and Solution 2 requires a light (electronic check) signature to a specific authorization by each user of the system.

The fourth example represents a Country with strict regulations, where solution 1 is not allowed at all and Solution 2 requires a written (or digital) signature to a specific authorization by each user of the system.

Country	Solution 1	Solution 2
Sample 1	Allowed. None,	--
Sample 2	Allowed. A change in the regulation of the Institution is necessary.	Allowed. Consensus-light
Sample 3	Not allowed.	Allowed. Consensus-light.

Appendix

Technical solutions for anonymization

When transferring anonymous data, the University can add a personal identifier which allows only the technicians of the University itself to trace the personal data of the data subject.
This identifier must be transferred together with the record and, if necessary, it makes the re-identification of the anonymized record possible.
For instance, this may occur when interviews on the employment status of graduates are carried out and researchers want to interview all the graduates of an academic/calendar year and not only the ones who have uploaded their CVs in the database.

Notice of privacy policy (Italy)

The students/graduates using the system receive two forms:
1. Consent (minimum) to the processing of the data needed for registration on the system. This consent is mandatory to at least be able to store the profile
2. Consent to the publication of the CV in the database. The user can still decide whether to make the CV visible to companies or not, but this consent is required to process the CV information associated with the administrative data.

Companies receive a different notice of privacy policy

Consent to registration

Section	Content
	The AlmaLaurea Inter-University Consortium guarantees that the processing of personal data complies with existing regulations. In compliance with article 13 of the Data Protection Code it states that: - the data are processed solely for the purpose of placement in the job market and vocational training; - the data requested below are processed solely for the purpose of user registration and to provide users a username and password to fill out the questionnaire; - the provision of data for registration is voluntary; - if consent is not granted, registration cannot be completed; - the data are processed using information technology; - data shall not be notified to third parties or be disclosed; the data subject can exercise the rights as per article 7 of the Data Protection Code, among which the right to confirmation, update and erasure of data by contacting the AlmaLaurea Inter-University Consortium, Viale Masini 36, 40126 Bologna, in writing; the independent data controllers are the AlmaLaurea Inter-University Consortium and the University where the title is attained. For purposes other than those related to the rights of the data subject, the data processor on behalf of the AlmaLaurea Inter-University Consortium is CINECA, via Magnanelli, 6/3 - 40033 Casalecchio di Reno (BO)

Consent to publication

Section	Content
	The AlmaLaurea Inter-University Consortium guarantees that the processing of personal data complies with existing regulations. In compliance with article 13 of the Data Protection Code it states that: - the data are processed solely for the purpose of placement in the job market and vocational training; - the data are processed using information technology to allow for searches with different keywords, such as the faculty and final score; - the data made anonymous are used also in aggregate form to generate statistical reports on high-school and university graduates; - the data highlighted in the questionnaire with a darker color are disseminated only in an aggregate form such that anonymity is guaranteed (e.g., questions on university experience, conditions of the family of origin, etc.); - the provision of data is voluntary; - the failure to fill out the questionnaire entails that the data not provided will not be loaded in the AlmaLaurea database. In this case, only the administrative data held by the University administration are loaded in the AlmaLaurea database in compliance with the provisions of the Data Protection Code; - the data subject must give a written communication that s/he does not intend to be entered in the AlmaLaurea database; - the data can be communicated to the AlmaLaurea S.r.l. Company (sole proprietorship company fully owned by the AlmaLaurea Inter-University Consortium, authorized to perform personnel selection activities by the Italian Welfare Ministry with authorization n°1517/RS of September 30, 2005), in the capacity of data processor, and to Italian and EU public and private entities and to trade associations, which expressly declare their interest in the data for job placement and vocational training purposes; - the data are communicated via the Internet; - the data will not be disseminated; the data subject can exercise the rights as per article 7 of the Data Protection Code, among which the right to confirmation, update and erasure of data by contacting the AlmaLaurea Inter-University Consortium, viale Masini 36, 40126 Bologna – Italy - Tel. +39 051 6088919 Fax +39 051 6088988. the independent data controllers are the AlmaLaurea Inter-University Consortium and the University where the title is attained. For purposes other than those related to the rights of the data subject, the data processor on behalf of the AlmaLaurea Inter-University Consortium is CINECA, via Magnanelli, 6/3 - 40033 Casalecchio di Reno (BO).

Consent to the processing of data for business users

	The AlmaLaurea Inter-University Consortium guarantees that the processing of personal data complies with existing regulations. In compliance with article 13 of the Data Protection Code it states that: the data are processed by the AlmaLaurea Inter-University Consortium, in the capacity of data controller, and by the AlmaLaurea S.r.l. Company, in the capacity of data processor, solely for the purpose of performing the contract and hence for the provision of the services offered by the AlmaLaurea Inter-University Consortium, which the enterprises belong to; - the data are processed on hardcopy and using information technology; - the provision of data is voluntary; - the failure to give the data marked with a star will prevent the execution and performance of the contract; - the provision of the data not marked with a star, though not instrumental to the execution of the contract, allows the AlmaLaurea Consortium to offer an efficient service to the contracting parties; - data will not be communicated to third parties save for the purposes related to the performance of the contract and the obligations of law and particularly those of an accounting and fiscal nature; - the data will not be disseminated; the contracting party can exercise the rights as per article 7 of the Data Protection Code, among which the right to confirmation, update and erasure of data by contacting the AlmaLaurea Inter-University Consortium, viale Masini 36, 40126 Bologna – Italy - Tel. +39 051 6088919 Fax +39 051 6088988.

Appendix – Details of the administrative data

Personal data

Structure		Description
Person		
	PersonName	First Name
	SecondName	Second Name / Parental Name
	PersonSurname	Last Name
	PersonName_local	First Name in local language (Arabic)
	PersonSecondName_local	Second Name / Parental Name in local language (Arabic)
	PersonSurname_local	Last Name in local language (Arabic)
	PersonGender	Gender
	PersonBirthDate	Date of birth
	PersonBirthPlace	City of Birth (code and name)
	PersonBirthProvince	Province of birth
	PersonBirthCountry	Country of birth
	PersonNationalIdentificationCode	National identification number (Es: CIN)
	PersonEnrollmentNumber	Student's Enrolment Number - Code National de Etudiant

Contacts

Structure			Description
Person			
Addresses			
	AddressCity		City
	AddressProvince		Province
	AddressCountry		Country
	AddressStreet		Address
	AddressZIP		ZIP code
Contacts			
	Contact		
		ContactType	Type of contact (email, fax, mobile, skype, …)
		ContactCategory	Category of the contact (home, work, parents).
		Contact	Content of the contact

Information on degree

Structure			Description
Person			
Addresses			
Contacts			
Degree			Degree information (node)
	DegreeCountry		Country where the degree has been obtained
	DegreeCode		Code of the degree inside the course database
	DegreeInternalCode		Code of the degree inside the university database (acrony
	DegreeTitle		Title of the degree
	DegreeCurriculum		Specific curriculum
	DegreeUniversity		University
	DegreeInstitute		Faculty/Department/Institute of reference for the course
	DegreeSite		Specific site location
	DegreeLevel		Level of the degree (1=License,2=Master,3=Doctorate,4=[
	DegreeType		Type of the degree
	DegreeClassification		Classification according to the national cathegories
	DegreeECTS		Number of ECTS (future use)
	DegreeModules		Number of modules
	DegreeLegalLength		Official (legal) length of the course of study (years)
	DegreeFinalMark		Final mark of the degree
	DegreeMention		Final Mention 1=Passable 2=A Bien 3=Bien 4=Trés Bien
	DegreeAverageExaminationMark		Average mark for the examinations
	DegreeEnrollmentDate		Date of start / Enrollment Date
	DegreeGraduationDate		Date of graduation/end of studies
	DegreeEnrollmentAcademicYear		Year of enrollment -
	DegreeModuleList		List of modules
		ModuleCode	code of the module
		ModuleTitle	Title of the module
		ModuleProfessor	Name of the professor
		ModuleMark	Examination mark for this module
		ModuleDate	Date of the examination for this module
		ModuleECTS	ECTS of the module
	DegreeInitialECTS		Number of ECTS at the beginning of the course of study
	DegreeInitialModules		Number of modules at the beginning of the course of study
	DegreeDissertation		
		DissertationTitle	Title of the dissertation
		DissertationCoordinator	Professor that coordinated the dissertation work
		DissertationSubject	Subject of the dissertation
		DissertationKeywords	Keywords for the disertation (comma separated list)
		DissertationAbstract	Abstract of the dissertation
		DissertationType	Type of dissertation (brief, research, stage, ...)

Information on prerequisite degree (if applicable)

Structure			Description
Person			
Addresses			
Contacts			
Degree			Degree information (node)
PrerequisiteDegree			Prerequisite degree (when appliable)
	PDegreeCountry		Country
	PDegreeCode		Code of the degree inside the course database
	PDegreeTitle		Title
	PDegreeUniversity		University
	PDegreeInstitute		Institute
	PDegreeLevel		Level of the degree (1=License,2=Master,3=Doctorate,4=D
	PDegreeType		Type of the degree
	PDegreeClassification		Classification according to the national cathegories

Information on high school

Structure			Description
Person			
Addresses			
Contacts			
Degree			Degree information (node)
PrerequisiteDegree			Prerequisite degree (when appliable)
HighSchoolDegree			High school degree
	HighSchollDegreeCode		Type of degree
	HighSchoolTitle		Title of the degree
	HighSchoolEndYear		Endyear of high school studies
	HighSchoolMark		Final mark of the degree
	HighSchoolCountry		Country where the high school has been attended

LAW OF THE REPUBLIC OF ARMENIA ON PERSONAL DATA

Adopted October 8, 2002

Chapter 1. General Provisions

ARTICLE 1. SUBJECT OF THE LAW REGULATION

1. This Law regulates relations connected with the processing of personal data by state and local self-governance bodies, state and community institutions, legal entities or natural persons.
2. This Law does not regulate relations connected with processing of personal data considered to be of state confidentiality, personal data published in public sources as well as processing of personal data by individuals for their personal, family or other matters of the type.

ARTICLE 2. THE ROA LEGISLATION ON PERSONAL DATA

1. The ROA Legislation on Personal Data consists of Constitution of the Republic of Armenia, this Law, other legislative acts regulating the processing of personal data.
2. If international treaties of the Republic of Armenia stipulate norms other than prescribed by this Law, the provisions of international treaties are applied.

ARTICLE 3. MAIN DEFINITIONS USED IN THE LAW

Main definitions used in this law have the following meanings:

a) Personal data: any data recorded on medium containing facts, events and circumstances about the person, in a form that allows or may allow to identify the person;
b) Processing of personal data: any function or group of functions related to the collection, inputting, systematization, modification, transfer, storage, correction, blocking, destroying and use of personal data;
c) Processor: state or local self-governance body, state or community institution, legal or natural person processing personal data;
d) Data subject: natural person to whom the personal data concern;
e) Personal data base (hereinafter data base): collection of personal data systematized with certain criteria;
f) Anonymous personal data: Any data on natural persons that don't allow identifying the person;
g) Confidential data: Data accessibility of which is restricted by law;
h) Blocking: Suspension of the possibility to transfer and use the personal data included in the personal database;
i) Third person: any subject other than the data subject or personal data processor.

CHAPTER 2. PROCESSING OF PERSONAL DATA

ARTICLE 4. MAIN PRINCIPLES OF PERSONAL DATA PROCESSING

1. Personal data are collected and processed legally.
2. Personal data are collected for clearly defined and declared legal purposes and shall not be used for other purposes, except the cases defined by law. Collection and processing of data that are not necessary for the achievement of the purpose of processing, is prohibited.
3. Personal data shall be kept for terms required by the objective they were collected and processed for, if the law does not envisage other procedures.

4. The personal data processors maintaining the database, except the state and local self-governance bodies, state and community institutions, define the regulations for the database maintenance.

ARTICLE 5. REGULATION FOR MAINTAINING THE DATABASE

1. The regulation for database maintenance includes the following information:

   1) Name of the processor and his/her whereabouts;

   2) Purpose and legal basis for personal data processing;

   3) List of personal data subject to processing;

   4) Categories of data subjects;

   5) Who may have access to personal data;

   6) Procedure for providing the data subject with information concerning him/her;

   7) Conditions and procedures for correcting, blocking and destroying personal data;

   8) Organizational and technical procedures for the protection of personal data

   9) Other information related to the personal data processing.

2. Definition of a regulation for the database maintenance is not obligatory:

   1) When the personal data are processed due to the request of state and local self-governance bodies, state and community institutions;

   2) When employers process personal data, due to procedures defined by legislation, on employment history of natural persons having work relations with employers.

ARTICLE 6. LEGALITY OF PERSONAL DATA PROCESSING

1. Processing of personal data is considered legal:

   1) When the personal data is processed with the consent of the data subject;

   2) When the personal data is processed for the protection of data subject's critical interests when there is no basis to assume that he/she will disagree when being informed about the processing;

   3) When processing of the personal data is envisaged by legislation or is necessary for execution of law requirements;

   4) When processing of the personal data is required for the protection of state and public security from immediate peril.

2. The consent of the data subject is the absolute voluntary permission to process his/her personal data expressed in any from.

   The data subject may withdraw his/her consent at any time. The withdrawal of the consent has no retrospective effect.

ARTICLE 7. PROCESSING OF PERSONAL DATA BY STATE AND LOCAL SELF-GOVERNANCE BODIES, STATE AND COMMUNITY INSTITUTIONS

1. State and local self-governance bodies, state or community institutions are entitled to process personal data in cases and due to the regulation prescribed by legislation.

2. State and local self-governance bodies, state or community institutions are obligated to ensure the authenticity of the personal data they process.

3. Procedure of sharing personal data between state and local self-governance bodies, state or community institutions is defined by the Government of the Republic of Armenia.

ARTICLE 8. ACCESSIBILITY OF PERSONAL DATA BASE

1. If the ROA laws do not envisage other procedures it is prohibited to limit:

1) Access to data bases maintained by state and community budgets, containing anonymous personal data on activities carried out by state and local self-governance bodies, state or community institutions, economic situation, needs of population, environment, sanitary-and-epidemiological situation, demography;

2) Access to library and archive documents containing personal data made anonymous by state and local self-governance bodies, state and community institutions being of public interest or necessary for the provision of population rights, freedoms or execution of responsibilities.

2. Access to personal databases mentioned under the clause 1 of this article is limited if databases contain data defined as confidential by ROA law.

ARTICLE 9. PROCESSING OF PERSONAL DATA WITH THE REQUEST OF A THIRD PARTY (CUSTOMER)

1. Personal data may be processed also with the request of a third person (customer). The request is submitted in a written form and it shall state legal basis and conditions, technical and organizational measures for the processing of personal data as well as other information envisaged by law necessary for definition of regulation for database maintenance.

2. Personal data are processed only in the frames of the request. The requestor is responsible for the processing of personal data in the frames of the request. If the request does not meet provisions of this Law or other legal acts regulating the processing of the personal data, the personal data processor shall inform the third party about it and refuse from processing the data.

3. The personal data is processed due to the procedure defined by article 7 of this Law when requested by state and local self-governance bodies, state or community institutions.

ARTICLE 10. LEGAL REGIME OF PERSONAL DATA

1. Personal data possessed by the processor are considered to be confidential information except cases envisaged by law.

2. The processor is obliged to undertake corresponding measures for the protection of databases containing personal data from sudden losses, illegal access to databases, illegal use of data.

3. Legal regime of personal data collected during activities of law-enforcing bodies is defined by law.

4. With the consent of the data subject or in cases envisaged by law information regime of general access may be established for the personal data (telephone information services, address books, biographical data, private announcements, declaration of incomes, etc.).

5. After the death of the data subject the legal regime of personal data is subject to modification with the regime of archive storage defined by legislation or other legal regime.

6. Protection of personal data of the deceased may be provided by other persons including protection of honor, dignity, reputation, as well as personal and family life by successors from illegal interference due to the procedure prescribed by law.

ARTICLE 11. INFORMATION PROVIDED TO THE DATA SUBJECT

1. Receiving the consent of the data subject the processor shall provide him/her with the following information:

    a) The purpose of personal data processing;
    b) Processor's name and location (address);
    c) Information on subjects to whom personal data will or may be provided;
    d) Personal data of general public accessibility.

2. With the request of the data subject the processor is obliged to provide the following information except the information defined under the clause 1 of this article:

    a) The fact of data subject's personal data processing;
    b) Contents and the source of processed personal data on the data subject;

    c) Basis for transferring personal data without the consent of the data subject.

The data subject is not obliged to substantiate the inquiry.

3. Information supplied to the data subject is provided free-of-charge, if not otherwise stated by the law.

4. Provision of information may be refused in cases defined by law.

ARTICLE 12. CORRECTING, BLOCKING AND DESTROYING PERSONAL DATA

1. The data subject may request the processor to make corrections in his/her personal data if there are corresponding documents confirming the incorrectness of personal data.

2. The personal data are blocked, when:

1) The data subject disagrees with the accuracy of his/her personal data or the legality of their processing;

2) It is requested by the data subject, whose personal data were processed with his/her consent;

3) The processor does not need them anymore for the accomplishment of the purpose they were processed for and the period defined by legislation for the storage of data has not expired.

Blocking of personal data is removed if there are no bases for blocking.

3. Personal data are destroyed, when:

1) Their processing does not meet the requirements of this law;

2) The processor does not need them anymore for the accomplishment of the purpose they were processed for and/or period defined by legislation for the storage of data has expired;

3) It is demanded by the data subject, whose personal data were processed with his/her consent.

4. Persons to whom personal data are regularly being transferred for future use shall be informed about personal data corrections, blocking and destroying.

ARTICLE 13. TRANSFER OF PERSONAL DATA TO THE FOREIGN COUNTRIES

Personal data are transferred to foreign countries according to international treaties of Armenia and on the basis stipulated under Articles 6 of this Law.

CHAPTER 3. ACCOUNT FOR INFRINGEMENT OF THE LAW

ARTICLE 14. APPEALING ACTIVITIES OF PERSONAL DATA PROCESSORS

1. If the data subject considers that illegal activities have been performed with his/her personal data he/she has the right of appealing these activities in the superiority or judicial order.

ARTICLE 15. ACCOUNT FOR INFRINGEMENT OF THE LAW

1. Those who infringe this legislation on personal data will be called to account according to the procedure defined by law.

CHAPTER 4. ENFORCEMENT OF THE LAW

ARTICLE 16. ENFORCEMENT OF THE LAW

This law becomes effective after 3 month of its promulgation.

RA President   R.Kocharyan

November 22, 2002

RA Law-422