REPUBLIC OF SAN MARINO

We the Captains Regent
of the Most Serene Republic of San Marino

Having regard to Article 4 of Constitutional Law no. 185/2005 and Article 6 of Qualified Law no. 186/2005;
Hereby promulgate and order the publication of the following Ordinary Law, approved by the Great and General Council during its sitting of 12 December 2018:

LAW no. 171 of 21 DECEMBER 2018

PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

CHAPTER I GENERAL PROVISIONS

TITLE I GENERAL PROVISIONS

Art.1
(Subject-matter and objectives)

1. This Law lays down rules relating to the protection of natural persons with regard to the processing of personal data, also held abroad, and rules relating to the free movement of such data.
2. This Law guarantees that the processing of personal data respects the data subject's fundamental rights and freedoms and human dignity, with particular regard to confidentiality, personal identity and the right to the protection of personal data.
3. Everyone shall have the right to the protection of personal data relating him or her.

Art. 2
(Definitions)

1. For the purposes of this Law:
a) "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier
such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
b) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

c) "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;
d) "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
e) "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
f) "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
g) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
h) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
i) "recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
l) "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
m) "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
n) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
o) "'genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
p) "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
q) "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
r) "enterprise" means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
s) "group of undertakings" means a group covering undertakings established and non-established in the territory of the Republic of San Marino, whereby the controlling undertaking can exert a dominant influence over the other undertakings and the other undertakings are directly or indirectly controlled or subject to the dominant influence of the controlling undertaking;
t) "binding corporate rules" means personal data protection policies which are adhered to by a controller or processor for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity, as referred to in Article 11 of Law no. 102 of 20 July 2004;
u) "supervisory authority" means an independent public authority responsible for ensuring compliance with the rules on the protection of personal data, i.e. the San Marino Data Protection Authority;
v) "information society service" means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
z) "international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more States;

aa) “public entities” means the entities falling within the definition of Administration, as defined by Law no.188 of 5 December 2011 ;
bb) "disclosure” means giving knowledge of personal data to one or more specified entities other than the data subject, by persons authorised to process personal data under the direct authority of the controller or processor or explicitly designated in accordance with Article 30, in whatever form, including by making them available, by consultation or combination;
cc) "dissemination” means giving knowledge of personal data to non-specified entities, in whatever form, also by making them available or by consultation.
2. Moreover, for the purposes of this Law:
a) "electronic communication" means any information exchanged or transmitted between a defined number of entities by means of a publicly available electronic communications service. Information transmitted to the public over an electronic communications network, as part of a broadcasting service, is excluded unless it is linked to an identified or identifiable subscriber or user;
b) “call” means a connection established by means of a publicly available electronic communications service allowing two-way voice communication;
c) “electronic communications networks” means transmission systems and, where applicable, switching or routing equipment and other resources, including non-active network elements, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;
d) “public communications network” means an electronic communication network used wholly or mainly for the provision of electronic communication services available to the public which support the transfer of information between network termination points;
e) “electronic communications services” means a service which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;
f) "subscriber" means any natural person, legal person, entity or association who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services, or otherwise any recipient of such services via prepaid cards;
g) "user" means any natural person using a publicly available electronic communications service, for private or commercial reasons, without necessarily having subscribed to this service;
h) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
i) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
l) “value added service” means any service which requires the processing of traffic data or location data other than traffic data beyond that which is necessary for the transmission of a communication or the billing thereof;
m) “electronic mail” means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

Art.3
(Territorial and material scope)

1. This Law shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Such processing is carried out by anyone established in the territory of the Republic of San Marino or in a place otherwise subject to the sovereignty of the Republic of San Marino.
2. This Law shall apply to the processing of personal data of data subjects who are in the Republic of San Marino by a controller or a processor not established in the Republic of San Marino, where the processing activities are related to:
a) the offering goods or services to such data subjects in the Republic of San Marino, irrespective of

whether connected to a payment; or
b) the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Republic of San Marino.
3. The processing of personal data by a natural person in the course of a purely personal or household activity shall be subject to the application of this Law only if the data are intended for systematic communication or dissemination.
4. This Law shall not apply to:
a) the processing of personal data carried out by public entities or by bodies that carry out tasks in the public interest, established or regulated by law, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, which will be governed by a specific delegated decree to be adopted within ninety days of the entry into force of this Law. Such delegated decree shall ensure that the exchange of personal data by the competent authorities for the purposes mentioned above is not limited or prohibited for reasons relating to the protection of natural persons with regard to the processing of personal data;
b) the processing of personal data when carrying out activities in relation to the foreign policy and national security;
c) the processing of personal data carried out by public entities or by bodies which carry out activities of public interest, established or regulated by law, for the purposes of international cooperation in tax matters.

TITLE II PRINCIPLES

Art.4
(Principles relating to processing of personal data)

1. Personal data shall be:
a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Articles 101 to 109, not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 101 to 109 subject to implementation of the appropriate technical and organisational measures required by this Law in order to safeguard the rights and freedoms of the data subject;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.
3. Information systems and computer software shall be configured to minimise the use of personal data and identification data, so as to exclude the processing when the purposes pursued in individual cases can be achieved by means of, respectively, anonymous data or appropriate methods that allow to identify the subject data concerned only when necessary.

Art.5
(Lawfulness of processing)

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
a) the data subject has given consent to the processing of his or her personal data for one or more

specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person, only if none of the other conditions of lawfulness laid down in this Article may be applied;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This provision shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Where the processing for a purpose other than that for which the personal data have been collected is not based on the conditions referred to in the previous paragraph, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia*:
a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 8, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Art.6
(Conditions for consent)

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Law shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
5. When the processing has multiple purposes, consent should be given for all of them.

Art.7
(Conditions applicable to child's consent in relation to information society services)

1. Where processing is based on consent, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Any information and communication, where processing is addressed to a child, should be

given by the controller in such a clear and plain language that the child can easily understand.

Art.8
(Processing of special categories of personal data)

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection, where appropriate safeguards for the fundamental rights and interests of the data subject exist;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, if such data are processed by or pursuant to contract with a health professional or another person also subject to an obligation of secrecy;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
l) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Articles 101 to 109, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. For the processing of data referred to in paragraph 1, in the cases mentioned in paragraph 2, the San Marino Data Protection Authority, by its own provision, may introduce measures of guarantee, without prejudice to the provisions of the "Declaration of the Rights of Citizens and Fundamental Principles of the San Marino Order, Law no. 59 of 8 July 1974 and subsequent amendments and integrations.
4. Such measures shall be adopted in relation to each category of personal data referred to in paragraph 1, paying particular attention to the specific purposes of the processing, and may provide for further conditions under which the processing of such data is allowed.
5. The personal data referred to in paragraph 1 may not be disseminated.

Art.9
(Processing of special categories of personal data necessary for reasons of substantial public interest)

1. Processing of the special categories of personal data referred to in Article 8, paragraph 1, necessary for reasons of substantial public interest, within the meaning of letter g), paragraph 2, of

the same Article shall be allowed if they are provided by the legislative provisions or regulations specifying the types of data that can be processed, the operations that can be carried out and the reasons for substantial public interest. These provisions shall, in any case, ensure:
a) that processing is proportionate to the aim pursued;
b) respect for the essence of the right to data protection;
c) specific measures to safeguard the fundamental rights and the interests of the data subject are provided for.
2. Without prejudice to the provisions of paragraph 1, processing shall be considered to be carried out for reasons of substantial public interest in the following areas or in other areas expressly identified by law:
a) access to administrative documents and civic access;
b) keeping of vital statistics records and registers, registries of the population residing in the Republic of San Marino and of San Marino citizens residing abroad, and of electoral lists, as well as issuance of identification documents or change of identity;
c) citizenship, immigration, asylum, foreigner's and refugee's status;
d) right to vote and to stand as a candidate and exercise of other political rights;
e) activities of public bodies aimed at the application, including through their authorities, of tax and customs provisions;
f) control and supervisory activities;
g) granting, payment, amendment and revocation of economic benefits, subsidies, donations, and other payments;
h) granting of honours and rewards, recognition of the legal personality of associations, foundations and bodies, including those of a religious nature, verification of the fit and proper and competence criteria to be met for appointments, assessment of competence profiles within the public administration, to offices, including those of a religious nature, and to managerial positions in legal entities, companies and non-state educational institutions, as well as the issuance and revocation of authorisations or licences, the granting of sponsorship, tutelage and representation awards, accession to honour committees and admission to ceremonies and institutional meetings;
i) relations between public bodies and third sector organisations;
l) sanctioning and protection activities at administrative or judicial level;
m) institutional relations with religious bodies, faiths and communities;
n) social welfare activities for the protection of children and persons in need, dependent and incapacitated;
o) processing of data revealing the health status by health professionals and health care bodies;
p) performance of the tasks of health care bodies, as well as in the fields of health and safety at work, public safety and health, civil protection, protection of life and physical integrity;
q) social protection of motherhood; dependencies; assistance, social integration and rights of disabled people;
r) education and training in school, professional education, higher education or university;
s) processing for historical purposes, concerning the conservation, codification and communication of documents held in the archives forming part of the documentary and archival heritage of the Republic referred to in Law No. 50 of 11 May 2012;
t) establishment, management and termination of employment relationships and other forms of employment, trade union matters, employment and compulsory placement, social security and assistance, protection of minorities and equal opportunities.

Art.10
(Processing of personal data relating to criminal convictions and offences)

1. Processing of personal data concerning criminal convictions and offences or related security measures on the basis of Article 5 paragraph 1, shall be carried out only under the control of official authority. In this case, reference shall be made to the current regulations on the criminal records, in coordination with the regulations on administrative documentation as per Law no. 159 of 5 October 2011, and on access to administrative documents as per Law no. 160 of 5 October 2011.

Art.11
(Processing which does not require identification)

1. If the purposes for which a controller processes personal data do not or do no longer require

the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Law.

2. Where, in cases referred to in paragraph 1, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

TITLE III
RIGHTS OF THE DATA SUBJECT

CHAPTER I
TRANSPARENCY AND MODALITIES

Art.12

(Transparent information, communication and modalities for the exercise of the rights of the data subject)

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and **33** relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

2. The rights provided for in Articles 15 to 22 shall be exercised by the data subject by means of a request addressed without formalities to the controller or processor, including through a person mandated by the controller. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11, paragraph 2, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Data Protection Authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

CHAPTER II
INFORMATION AND ACCESS TO PERSONAL DATA

Art.13

(Information to be provided where personal data are collected from the data subject)

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of Article 5, paragraph 1, the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to transfer personal data to a foreign country or international organisation and the possibility of freely transfer data as referred to in Article 46, or in the case of the transfers referred to in Article 47 or 48, or to Article 50, paragraph 2, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability under Article 20;

c) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to report or to lodge a complaint with the Data Protection Authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, referred to in Article 22, paragraphs 1 and 4 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Art.14

(Information to be provided where personal data have not been obtained from the data subject)

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, that the controller intends to transfer personal data to a recipient in a foreign

country or to an international organisation and the possibility of freely transfer data as referred to in Article 46, or in the case of transfers referred to in Article 47 or 48, or paragraph 2 of Article 50, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point (f) of Article 5, paragraph 1, the legitimate interests pursued by the controller or by a third party;

c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

d) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to report or to lodge a complaint with the Data Protection Authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, referred to in Article 22, paragraphs 1 and 4 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1, 2, e and 4 shall not apply insofar as:

a) the data subject already has the information;

b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Articles 101 to 109 or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; or

c) where the personal data must remain confidential subject to an obligation of professional secrecy, including a statutory obligation of secrecy.

Art.15

(Right of access by the data subject)

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in foreign countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such

processing;
f) the right to report or to lodge a complaint with the Data Protection Authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22, paragraphs 1 and 4 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a foreign country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 47 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

CHAPTER III
RECTIFICATION AND ERASURE

Art.16
(Right to rectification)

1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Art.17
(Right to erasure, "right to be forgotten")

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based, where there is no other legal ground for the processing
c) the data subject objects to the processing pursuant to Article 21, paragraph 1 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21, paragraph 2;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 7, paragraph 1.
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health in accordance with Article 8, paragraph 2, letter h) and i) as well as Article **8**, paragraph 3;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 101 to 109, in so far as the right referred to in

paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.

Art.18
(Right to restriction of processing)

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Art.19
(Notification obligation regarding rectification or erasure of personal data or restriction of processing)

1. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17, paragraph 1 and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Art. 20
(Right to data portability)

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
a) the processing is based on consent or on a contract; and
b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

CHAPTER IV
RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Art. 21
(Right to object)

1. The data subject shall have the right to object, on grounds relating to his or her particular

situation, at any time to processing of personal data concerning him or her which is based on letters e)or f) of paragraph 5, Article **5**, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

3. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

4. In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.

5. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Articles 101 to 109, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Art. 22

(Automated individual decision-making, including profiling)

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is based on the data subject's explicit consent.

3. In the cases referred to in paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article **8** paragraph 1, unless point a) or g) of Article **8**, paragraph 2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Art. 23

(Restrictions to the data subject's rights)

1. The rights referred to in Articles 15 to 22 may not be exercised with a request to the controller or processor or with a complaint to the Data Protection Authority where the exercise of these rights may adversely affect:

a) the interests protected under the provisions on money laundering;

b) the interests protected under the provisions on support for victims of extortion;

c) the work of Parliamentary Commissions of Inquiry;

d) the activities carried out by a public body on the basis of a specific legal provision, only for purposes relating to monetary and exchange rate policy, the payment system, the supervision of intermediaries and credit and financial markets, and the protection of their stability;

e) the exercise of a right in judicial proceedings.

2. In the cases referred to in paragraph 1, letters a), b), d) and e), the rights referred to in the same paragraph shall be exercised in accordance with the legal or regulatory provisions governing the sector, which shall at least contain measures to regulate the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer, the specification of the controller or categories of controllers, the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing, the risks to the rights and freedoms of data subjects and the right of data subjects to be informed about the restriction, unless

that may be prejudicial to the purpose of the restriction.
3. The exercise of such rights may, in any event, be delayed, limited or excluded by reasoned communication and given to the data subject without delay, for as long as, and to the extent that, this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to safeguard the interests referred to in letters a), b), d) and e) of paragraph 1. In such cases, the rights of the data subject may also be exercised through the Data Protection Authority pursuant to the modalities referred to in Article 63. In this case, the Data Protection Authority shall inform the data subject that it has carried out all the necessary controls or that it has carried out a review, as well as the right of the data subject to seek judicial remedy. The controller shall inform the data subject of the possibilities provided for by this paragraph.

Art. 24
(Restrictions for reasons of justice)

1. With regard to the processing of personal data in the context of proceedings before the Judicial Authority, in order to protect judicial independence and judicial proceedings, the rights and obligations referred to in Articles 12 to 22 and 35 shall be governed in accordance with the legal or regulatory provisions relating to such proceedings, which shall at least contain measures to regulate the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer, the specification of the controller or categories of controllers, the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing, the risks to the rights and freedoms of data subjects and the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.
2. Without prejudice to the provisions of paragraph 1, the exercise of the rights and the performance of the obligations laid down in Articles 12 to 22 and 35 may be delayed, limited or excluded, by reasoned communication given without delay to the data subject, to the extent and for the duration that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to protect judicial independence and judicial proceedings.
3. In such cases, the rights of the data subject may also be exercised through the Data Protection Authority pursuant to the modalities referred to in Article 63. In this case, the Data Protection Authority shall inform the data subject that it has carried out all the necessary controls or that it has carried out a review, as well as the right of the data subject to seek judicial remedy. The controller shall inform the data subject of the possibilities provided for by this paragraph.

Art. 25
(Rights of deceased persons)

1. The rights referred to in Articles 15 to 22 relating to personal data of deceased persons may be exercised by those who have a personal interest, or act for the protection of the data subject, as their heir or agent, or for family reasons worthy of protection.
2. The exercise of the rights referred to in paragraph 1 shall not be permitted in the cases provided for by law or when, only in relation to the offer of information society services, the data subject has expressly prohibited it in a written declaration submitted to the controller.
3. The data subject's will to prohibit the exercise of the rights referred to in paragraph 1 shall be specific, free and informed; such prohibition may concern the exercise of only some of the rights referred to in that paragraph.
4. The data subject shall have the right to withdraw or modify the prohibition referred to in paragraphs 2 and 3 at any time.
5. In any event, the prohibition may not have any detrimental effect on the exercise by third parties of their property rights, arising from the death of the data subject or of their right to defend their interests before a court.

TITLE IV
CONTROLLER AND PROCESSOR

CHAPTER I
GENERAL OBLIGATIONS

Art. 26
(Responsibility of the controller)

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 41 or approved certification mechanisms as referred to in Article 43 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Art. 27
(Data protection by design and by default)

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Law and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 43 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

Art. 28
(Joint controllers)

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Law, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Law in respect of and against each of the controllers.

Art. 29
(Processor)

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a foreign country or an international organisation, unless required to do so by a special law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) takes all measures required pursuant to Article 33;
d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Title III of this Section;
f) assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 37 taking into account the nature of processing and the information available to the processor;
g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless special laws require storage of the personal data; and
h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. In this case, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Law or other data protection provisions.
4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Law. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 43 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4.
6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraph 7.
7. The Data Protection Authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4.
8. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.
9. Without prejudice to the rules referred to in Title VIII of this Section, if a processor infringes this Law by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Art.30

(Processing under the authority of the controller or processor)

1. The controller or processor may provide, within their organisational structure, that specific tasks and functions relating to the processing of personal data are to be assigned to expressly designated natural persons acting under their authority.
2. The controller or processor shall identify the most appropriate ways of authorising the processing of personal data by persons acting under their direct authority.
3. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by special laws.

Art.31

(Records of processing activities)

1. Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a foreign country or an international organisation, including the identification of that foreign country or international organisation and, in the case of transfers referred to in the paragraph 2 of Article 50, the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32, paragraph 1.
2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
b) the categories of processing carried out on behalf of each controller;
c) where applicable, transfers of personal data to a foreign country or an international organisation, including the identification of that foreign country or international organisation and, in the case of transfers referred to in the paragraph 2 of Article 50, the documentation of suitable safeguards;
d) where possible, a general description of the technical and organisational security measures referred to in Article 32, paragraph 1.
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 8 paragraph 1 or personal data relating to criminal convictions and offences referred to in Article 10.

Art.32

(Cooperation with the Data Protection Authority)

1. The controller and the processor shall cooperate, on request, with the Data Protection Authority in the performance of its tasks.

CHAPTER II
SECURITY OF PERSONAL DATA

Art.33
(Security of processing)

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 41 or an approved certification mechanism as referred to in Article 43 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by special laws.

Art.34
(Notification of a personal data breach to the supervisory authority)

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Data Personal Data Protection to verify compliance with this Article.

Art.35
(Communication of a personal data breach to the data subject)

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of

natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 34, paragraph 3.

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the Data Protection Authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

CHAPTER III
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Art.36
(Data protection impact assessment)

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of data referred to in Article 8 paragraph 1, or of personal data relating to criminal convictions and offences referred to in Article 10; or

c) a systematic monitoring of a publicly accessible area on a large scale.

4. The Data Protection Authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The Data Protection Authority may establish and make public a list of the types of processing operations which are not subject to the requirement for a data protection impact assessment.

6. The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law taking into account the rights and legitimate interests of data subjects and other persons concerned.

7. Compliance with approved codes of conduct referred to in Article 41 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data

protection impact assessment.
8. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
9. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Art.37
(Prior consultation)

1. The controller shall consult the Data Protection Authority to processing where a data protection impact assessment under Article 36 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the Data Protection Authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Law, in particular where the controller has insufficiently identified or mitigated the risk, the Authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 59. That period may be extended by six weeks, taking into account the complexity of the intended processing. The Data Protection Authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.
3. When consulting the Data Protection Authority pursuant to paragraph 1, the controller shall provide the Authority with:
a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
b) the purposes and means of the intended processing;
c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Law;
d) where applicable, the contact details of the data protection officer;
e) the data protection impact assessment provided for in Article 36; and
f) any other information requested by the supervisory authority.
4. The Congress of State and the Great and General Council shall consult the Data Protection Authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing of personal data, in order to obtain a prior opinion.

CHAPTER IV
DATA PROTECTION OFFICER

Art.38
(Designation of the data protection officer)

1. The controller and the processor shall designate a data protection officer in any case where:
a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 8 and personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.
5. The data protection officer may act for such associations and other bodies representing controllers or processors. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 40.
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Data Protection Authority.

Art.39
(Position of the data protection officer)

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 40 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Law.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.
6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Art.40
(Tasks of the data protection officer)

1. The data protection officer shall have at least the following tasks:
a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Law and to other data protection provisions;
b) to monitor compliance with this Law, with other data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 36;
d) to cooperate with the Data Protection Authority; and
e) to act as the contact point for the Data Protection Authority on issues relating to processing, including the prior consultation referred to in Article 37, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

CHAPTER V
CODES OF CONDUCT AND CERTIFICATION

Art.41
(Codes of conduct)

1. Associations and other bodies representing categories of controllers or processors may prepare or amend or extend codes of conduct, taking account of the specific features of the various

processing sectors and the specific needs of micro, small and medium-sized enterprises, for the purpose of specifying the application of this Law. Codes of conduct shall be intended to contribute to the proper application of this Law, with regard to:

a) fair and transparent processing;
b) the legitimate interests pursued by controllers in specific contexts;
c) the collection of personal data;
d) the pseudonymisation of personal data;
e) the information provided to the public and to data subjects;
f) the exercise of the rights of data subjects;
g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
h) the measures and procedures referred to in Articles 26 and 27 and the measures to ensure security of processing referred to in Article 33;
i) the notification of personal data breaches to the Data Protection Authority and the communication of such personal data breaches to data subjects;
l) the transfer of personal data to foreign countries or international organisations; or
m) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Title VIII of this Section.

2. Associations and other bodies which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the Data Protection Authority. The Data Protection Authority shall provide an opinion on whether the draft code, amendment or extension complies with this Law and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

3. Where the draft code, or amendment or extension is approved in accordance with paragraph 51, the Data Protection Authority shall publish the code on its website.

4. A code of conduct referred to in paragraph 2 shall contain mechanisms which enable the body referred to in Article 42 to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the Data Protection Authority pursuant to Article 58 and 59.

Art.42

(Monitoring of approved codes of conduct)

1. Without prejudice to the tasks and powers of the Data Protection Authority, the monitoring of compliance with a code of conduct pursuant to Article 41 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Data Protection Authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Data Protection Authority;
b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
d) demonstrated to the satisfaction of the Data Protection Authority that its tasks and duties do not result in a conflict of interests.

3. Without prejudice to the tasks and powers of the Data Protection Authority and the provisions of Chapter VIII of this Section, a body as referred to in paragraph 1 shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the Data Protection Authority of such actions and the reasons for taking them.

4. The Data Protection Authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Law.

5. This Article shall not apply to processing carried out by public authorities and bodies.

Art.43
(Certification)

1. The controller or processor may submit its processing to a data protection certification mechanism, to data protection seals and marks for the purpose of demonstrating compliance with this Law of the processing operations carried out by the same controllers and processors.
2. The certification shall be voluntary, available via a process that is transparent and shall be issued by the certification bodies referred to in Article 44, either national or foreign, on the basis of criteria approved pursuant to Article 59.
3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 44 with all information and access to its processing activities which are necessary to conduct the certification procedure.
4. A certification pursuant to this Article shall not reduce the responsibility of the controller or the processor for compliance with this Law and shall be without prejudice to the tasks and powers of the Data Protection Authority pursuant to Article 58 or 59.
5. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn by the certification bodies which has issued it where the requirements for the certification are not or are no longer met.

Art.44
(Certification bodies)

1. Without prejudice to the tasks and powers of the Data Protection Authority, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the Data Protection Authority in order to allow it to exercise its powers pursuant to point (h) of Article 59, paragraph 2 where necessary, issue and renew certification.
2. Certification bodies shall be accredited by the Data Protection Authority only where they have:
a) demonstrated their independence and expertise in relation to the subject-matter of the certification;
b) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
c) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
d) demonstrated, to the satisfaction of the Data Protection Authority, that their tasks and duties do not result in a conflict of interests.
3. The certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Law.
4. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in paragraph
5. The certification body shall provide the Data Protection Authority with the reasons for granting or withdrawing the requested certification.
6. Without prejudice to Chapter VIII, the Data Protection Authority shall revoke an accreditation of a certification body, where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Law.

TITLE V
TRANSFERS OF PERSONAL DATA TO OTHER COUNTRIES OR INTERNATIONAL ORGANISATIONS

Art. 45
(General principle for transfers)

1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a foreign country or to an international organisation shall take place only if, subject

to the other provisions of this Law, the conditions laid down in this Title are complied with by the controller and processor, including for onward transfers of personal data from the foreign country or international organisation to another foreign country or to another international organisation. All provisions in this Title shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Law is not undermined.

Art. 46
(Transfer of data to foreign countries)

1. A transfer of personal data from and to all Member States, as well as to all foreign countries may take place where the Commission has adopted an adequacy decision with regard to those foreign countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Such a transfer shall not require any specific authorisation.
2. A transfer of personal data may also take place from and to all foreign countries with which the Republic of San Marino has signed bilateral agreements or treaties providing for the exchange of personal data and governing the safeguards in relation to the processing of personal data in accordance with this Law. Such a transfer shall not require any specific authorisation.

Art.47
(Transfers subject to appropriate safeguards)

1. Except in the cases referred to in Article 46, a controller or processor may transfer personal data to a foreign country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the Data Protection Authority, by:
a) a legally binding and enforceable instrument between public authorities or bodies;
b) binding corporate rules in accordance with Article 48, as well as those adopted by the European Commission;
c) standard data protection clauses adopted by the Data Protection Authority, as well as those adopted by the European Commission;
d) an approved code of conduct pursuant to Article 41 together with binding and enforceable commitments of the controller or processor in the foreign country to apply the appropriate safeguards, including as regards data subjects' rights; or
e) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. Subject to the authorisation from the Data Protection Authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the foreign country or international organisation; or
b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Art. 48
(Binding corporate rules)

1. The Data Protection Authority shall approve binding corporate rules, provided that they:
a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
c) fulfil the requirements laid down in paragraph 2.
2. Binding corporate rules shall specify at least:
a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
b) the data transfers or set of transfers, including the categories of personal data, the type of

processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
c) their legally binding nature, both internally and externally;
d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the Data Protection Authority and before the competent courts in accordance with Title VII of this Section, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
f) the acceptance by the controller or processor of liability for any breaches of the binding corporate rules by any member concerned not established in the Republic of San Marino; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) is provided to the data subjects in addition to Articles 13 and 14;
h) the tasks of any data protection officer designated in accordance with Article 36 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
i) the complaint procedures;
l) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Data Protection Authority;
m) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Data Protection Authority;
n) the cooperation mechanism with the Data Protection Authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the Data Protection Authority the results of verifications of the measures referred to in point (l);
o) the mechanisms for reporting to the Data Protection Authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a foreign country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
p) the appropriate data protection training to personnel having permanent or regular access to personal data.

Art.49
(Recognition of judgements and decisions of foreign counties)

1. Any judgement of a court or tribunal and any decision of an administrative authority of a foreign country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting foreign country and the Republic of San Marino, without prejudice to other grounds for transfer pursuant to this Chapter.

Art.50
(Derogations for specific situations)

1. Except in the cases referred to in Article 46 or in the absence of appropriate safeguards pursuant to Article 47, including binding corporate rules, a transfer or a set of transfers of personal data to a foreign country or an international organisation shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which is intended to provide information to the public and which can be consulted by the public at large and by any person who can demonstrate a legitimate interest, only provided that the requirements for consultation laid down in special rules are met. However, a transfer may not involve the entirety of the personal data or entire categories of the data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer may take place only at the request of those persons or if they are to be the recipients.

2. Where a transfer could not be based on a provision in Article 47 or 48 and none of the derogations for a specific situation referred to in paragraph 1 is applicable, a transfer to a foreign country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the Data Protection Authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

3. Points (a), (b) and (c) of the paragraph 1 and paragraph 2 shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The controller or processor shall document the assessment as well as the suitable safeguards referred to in paragraph 2 in the records referred to in Article 31.

Art.51
(International cooperation for the protection of personal data)

1. In relation to foreign countries and international organisations, the Data Protection Authority shall take appropriate steps to:
a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with foreign countries;
e) promote memorandum of understanding and agreements with the competent supervisory authorities of foreign countries.

TITLE VI
SAN MARINO DATA PROTECTION AUTHORITY

CHAPTER I
THE AUTHORITY

Art.52
(San Marino Data Protection Authority - Appointment and composition)

1. San Marino Data Protection Authority is hereby established as an independent public authority responsible for monitoring the application of this Law in order to protect the fundamental rights and freedoms of natural persons in respect of personal data processing.
2. The Data Protection Authority shall be a collegiate body composed of the Panel and the Office. The Panel shall be made up of three members appointed by the Great and General Council, who meet the requirements referred to in Article 53. At the time of the appointment of the Panel, the Great and General Council shall identify the President and the Vice-President.
3. Members shall remain in office for four years and may be renewed only once; their term of office shall expire on expiry of the mandate or in the case of voluntary resignation or measure adopted *ex officio*.
4. A member shall be removed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties as laid down in Articles 53 and 54.
5. Members of the Data Protection Authority shall be subject to a duty of professional secrecy both during and after their term of office with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers.
6. The Data Protection Authority may have its own organisational structure, namely the Data Protection Office, whose staffing needs are established and, subsequently, modified with a specific delegated decree, without prejudice to the principles referred to in Article 55.

Art.53
(Fit and proper requirements of the members of the Data Protection Authority)

1. Members of the Data Protection Authority shall meet the following fit and proper requirements:
a) having never been finally convicted, without prejudice to rehabilitation effects, of crimes against public order, public faith or by private individuals against public administration;
b) having never been finally convicted, without prejudice to rehabilitation effects, of other crimes, for which imprisonment without suspension for a period of not less than two years has been applied;
2. Fit and proper requirements shall also include the absence of equivalent final convictions handed down in jurisdictions other than San Marino.
3. In addition, members of the Data Protection Authority shall be chosen from among experts having proven experience and competence in the field of personal data protection, with particular reference to legal matters and information technology.

Art.54
(Autonomy and independence)

1. The Data Protection Authority shall act with complete autonomy and independence in performing its tasks and exercising its powers in accordance with this Law.
2. The Data Protection Authority shall be provided with the human, technical and financial resources necessary for the effective performance of its tasks and exercise of its powers.
3. Members of the Data Protection Authority, in the performance of their tasks and exercise of their powers in accordance with this Law, shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
4. Members of the Data Protection Authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any professional or advisory activity in the Republic of San Marino nor be directors or employees of public or private bodies, nor hold elected offices. Failure to comply with this provision shall entail dismissal of the member.
5. The provisions of Law no. 141 of 5 September 2014 shall apply to the Data Protection Authority, insofar as they are compatible.

Art.55
(Data Protection Office)

1. The Data Protection Office shall be headed by a Director in possession of a Master's Degree in Law.
2. Job specifications of employees shall be laid down in the delegated decree referred to in Article 52, paragraph 6.

3. With its own regulation, the Data Protection Authority shall define the organization and functioning of the Office, also to carry out the tasks referred to in Article 58. The regulation shall be published on the website of the Data Protection Authority.
4. The Office of the Data Protection Authority shall be subject to the principles and rules of public employment and employment relationships by the State. The principles and rules of Law no. 188 of 5 December 2011 and its subsequent amendments and integrations shall also apply to the Office of the Authority, insofar as they are compatible.
5. The Data Protection Authority may avail itself of the services of consultants on the occasion of complex or delicate technical or legal issues. Relations with consultants shall be regulated by fixed-term contracts of no more than one year's duration.
6. Employees of the Data Protection Office and consultants shall be bound by professional secrecy, both during and after their term of office.
7. The staff of the Data Protection Office in charge of the verifications defined in the following articles may rely on judicial police officers.
8. In the State budget, a special chapter shall be set up for the operating expenses of the Data Protection Authority.
9. Every year, the Data Protection Authority shall draw up the report on financial management, which shall be subject to control by the Commission for the Control of Public Finance.

Art.56
(Applicable principles)

1. Documents produced or received by the Data Protection Authority shall be subject to the legislation on access to administrative documents as per Law No. 160 of 5 October 2011 and subsequent amendments and integrations.

CHAPTER II
COMPETENCE, TASKS AND POWERS

Art. 57
(Competence)

1. The Data Protection Authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it by this Law on the territory of the Republic of San Marino.
2. The Data Protection Authority shall not be competent to supervise processing operations of courts acting in their judicial authority.
3. The Data Protection Authority shall cooperate with the other supervisory authorities concerned by exchanging relevant information and providing mutual assistance in order to implement and enforce this Law. On special issues the Authority shall refer to the other supervisory authorities concerned to obtain their opinion.

Art. 58
(Tasks)

1. Without prejudice to the other tasks indicated in this Law, the Data Protection Authority shall have the following tasks:
a) monitor and enforce the application of this Law;
b) promote a culture of personal data protection in all areas and with any initiative and activity, including with regard to data subjects and data processors, relating to the obligations provided for by this Law;
c) advise the Great and General Council, the Congress of State and other bodies and institutions on legislative and administrative measures relating to the protection of the rights and freedoms of natural persons with regard to processing;
e)upon request, provide information to any data subject concerning the exercise of their rights under this Law and, if appropriate, cooperate with the supervisory authorities in foreign countries to that end;
f) examine and handle complaints lodged by data subjects or their representative associations;
g) facilitate activities regarding the protection of personal data by making useful documents and

materials available to users on a specific area of the institutional website;
h) cooperate with, including sharing information with other supervisory authorities of foreign countries;
i) conduct investigations on the application of this Law, including on the basis of information received from another public authority;
l) monitor technological innovation, developments of information and communication technologies and commercial practices with regard to the potential impact on the protection of personal data;
m) adopt standard contractual clauses referred to in Article 29, paragraph 7 and Article 47, paragraph 2, letter d);
n) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 36, paragraph 4;
o) give advice on the processing operations referred to in Article 37, paragraph 2;
p) encourage the drawing up of codes of conduct pursuant to Article 41, paragraph 1 and provide an opinion and approve such codes of conduct which provide sufficient safeguards pursuant to Article 41, paragraph 3;
q) encourage and monitor beforehand the establishment of data protection certification mechanisms as well as data protection seals and marks pursuant to Article 43, paragraph 1, and approve the certification criteria pursuant to Article 43, paragraph 2;
r) monitor the correct application of the certifications in accordance with Article 43;
s) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 42 and of a certification body referred to in Article 44, and accredit it accordingly;
t) authorise contractual clauses and provisions referred to in Article 47, paragraph 3;
u) approve binding corporate rules pursuant to Article 48;
v) keep internal records of infringements of this Law and of measures adopted in accordance with Article 59 paragraph 2; and
z) fulfill any other tasks related to the protection of personal data.
2. The performance of the tasks of the Data Protection Authority shall be free of charge for the data subject and, where applicable, for the data protection officer in the event of complaints. The amount of the fee to be paid in the event of complaints to be lodged to the Authority shall be determined by delegated decree.
3. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The Data Protection Authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 59
(Powers)

1. The Data Protection Authority shall have the following investigative powers:
a) to order the controller and the processor to provide any information it requires for the performance of its tasks;
b) to carry out investigations in the form of data protection audits;
c) to notify the controller or the processor of an alleged infringement of this Law;
d) to obtain from the controller or the processor access to all personal data and all information necessary for the performance of its tasks; and
e) to obtain access to any premises of the controller and the processor, including databases, archives and all data processing equipments and means.
2. The Data Protection Authority shall have the following corrective powers:
a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Law;
b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Law;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Law;
d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
e) to order the controller to communicate a personal data breach to the data subject;
f) to impose a temporary or definitive limitation including a ban on processing;
g) to order the rectification or erasure of personal data or restriction of processing pursuant to

Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17, paragraph 2 and Article 19;
h) to order the certification body to withdraw the certificate issued pursuant Articles 43 and 44 and order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
i) to impose an administrative fine pursuant to Title VIII of this Part, in addition to, or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case; and
l) to order the suspension of data flows to a recipient in a foreign country or to an international organisation.
3. The Data Protection Authority shall have the following authorisation and advisory powers:
a) to advise the controller in accordance with the prior consultation procedure referred to in Article 37;
b) to issue, on its own initiative or on request, opinions addressed to the Great and General Council, to the Congress of State, or to other bodies and institutions as well as to the public on any issue related the protection of personal data;
c) to issue an opinion and approve draft codes of conduct in accordance with Article 41, paragraph 3;
d) to accredit certification bodies pursuant to Article 43;
e) to approve criteria of certification in accordance with Articles 43 and 44;
f) to adopt standard data protection clauses referred to in Article 29, paragraph 7 and Article 47, paragraph 2, letter d);
g) to authorise contractual clauses referred to in Article 47, paragraph 3, letter a);
h) to authorise administrative arrangements referred to in Article 47, paragraph 3, letter b);
i) to approve binding corporate rules in accordance with Article 48;
l) to authorise the establishment of new databases of the State and public entities, subject to a favourable opinion by the competent body.
4. The Data Protection Authority shall have the power to bring infringements of this Law to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Law.

Art.60
(Request for information and production of documents)

1. Within the scope of the powers referred to in article 59, and for the performance of its duties, the Data Protection Authority may request the controller, the processor, the data subject or even third parties to provide information and to produce documents also on the content of databases.

Art.61
(Verifications)

1. The Data Protection Authority may provide access to databases, archives or other inspections and checks in the premises where the processing takes place or where it is necessary to carry out verifications useful to monitor compliance with the rules on the processing of personal data.
2. The verifications referred to in paragraph 1 shall be carried out by the staff of the Office of the Data Protection Authority.
3. The Data Protection Authority shall also rely, where necessary, upon the collaboration of other State bodies for the performance of its institutional tasks.
4. The verifications referred to in paragraphs 1 and 2, if carried out in a dwelling or other place of private residence or in the property concerned, shall be carried out with the informed consent of the controller or processor. In case of lack of such consent, verifications shall be authorized by the judicial authority, which, if the urgency of the verification is documented, shall issue a motivated decree without delay from the receipt of the request by the Data Protection Authority.
5. By applying the safeguards, referred to in paragraph 4, the verifications carried out as referred to in the same paragraph may also relate to publicly accessible communications networks, as data and information may be acquired online. To this end, if the verifications are carried out at the controller's premises, a specific verbatim record shall be drawn up jointly with the parties.

Art.62
(Modalities)

1. The operating staff, provided with an identification document, may be assisted, where necessary, by consultants bound to secrecy on what has come to their knowledge in the exercise of their functions, with regard to information that must remain secret. When carrying out verifications and technical operations, the staff may also take copies of any record, datum and document, including on a sample basis and electronically. A summary verbatim record of the verifications shall be drawn up, where any statements made by the parties shall also be recorded.
2. A copy of the authorisation of the judicial authority, if issued, shall be given to the controllers subject to verification. Such controllers shall be required to have them carried out and to provide the necessary collaboration for this purpose. In case of refusal, the verifications shall be carried out in any case and the costs incurred shall be charged to the controller on the bases of the measure ordering the verification.
3. The verifications, if carried out at the premises of the controller or the processor shall be carried out by informing the controller or, if the controller is absent or not designated, the persons authorised to process personal data under the direct authority of the controller or the processor or expressly designated in accordance with Article 30. Persons designated by the controller or the processor may attend the verification operations.
4. The information, requests and measures referred to in this Article and in Articles 60 and 61 may also be transmitted by qualified electronic certified delivery services.

Art.63
(Special verifications)

1. For the processing of personal data referred to in Article 77, the verifications shall be carried out by a member designated by the Data Protection Authority.
2. If the processing does not comply with the provisions of the law, the Data Protection Authority shall inform the controller or the processor of the necessary changes and additions to be implemented and shall verify their implementation. If the verification has been requested by the data subject, he/she shall be provided in any case with feedback on the outcome of the verification, if this does not prejudice actions or operations to protect public order and security or the prevention and suppression of criminal offences or if there are grounds for State defence or security.
3. Verifications shall not be delegated. When necessary because of the specific nature of the verification, the designated member may be assisted by specialised staff who are bound to secrecy about what they have learned on information which must remain secret. The records and documents acquired are kept in such a way as to ensure their secrecy and the President and members of the Data Protection Authority may have access to them.
4. For the verifications referred to in paragraph 3 relating to data covered by State secrecy, the designated member shall examine the relevant records and documents and orally report in the meetings of the Data Protection Authority.
5. The validity, effectiveness and usability of records, documents and measures in the judicial proceeding based on the processing of personal data, which do not comply with legal or regulatory provisions, shall remain governed by the relevant procedural provisions in civil and criminal matters.

Art.64
Activity reports

1. The Data Protection Authority shall draw up an annual report on its activities and on the state of implementation of this Law, which may include a list of types of infringement notified and types of measures taken in accordance with Article 59, paragraph 2. The report shall be transmitted to the Great and General Council, the Congress of State and the Captains Regent. It shall be made available to the public.

TITLE VII
PROTECTION OF THE DATA SUBJECT

Art.65
(Remedies)

1. Remedies to enable data subjects to exercise their rights shall be administrative protection and judicial protection as provided for in the following Articles.
2. Data subjects shall exercise their rights to administrative protection through complaints and reports to the Data Protection Authority.
3. The judicial protection with regard to personal data shall be governed by Article 70.

Art.66
(Complaint)

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Data Protection Authority, if the data subject considers that the processing of personal data relating to him or her infringes this Law, if the alleged infringements has taken place in the Republic of San Marino.
2. The complaint shall contain a most detailed possible indication of the facts and circumstances on which it is based, the provisions allegedly infringed and the measures required, as well as the identification details of the controller, of the processor, if known.
3. Complaint, signed by data subjects or, on their behalf, by the lawyer or by a body, organisation or association active in the field of personal data protection, shall be accompanied by any documentation that may be useful for the purposes of its evaluation.
4. The complaint shall be lodged with the Data Protection Authority by registered mail with acknowledgement of receipt, by the qualified electronic delivery service, or through the online procedure on the website of the Data Protection Authority.
5. The Data Protection Authority shall prepare the form that can be used for complaints, to be published on its website; with its own regulations it shall also regulate the procedure for handling the complaints, as well as simplified procedures for handling complaints relating to the infringement of Articles 15 to 22.

Art.67
(Decision on the complaint)

1. After the verification phase has been completed, if the complaint is not manifestly unfounded and there are grounds for adopting a measure, the Data Protection Authority may adopt the measures referred to in Article 59 even before the closure of the procedure.
2. The Data Protection Authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 70.
3. After the verification phase has been completed, the Data Protection Authority shall decide thereon by its own motivated measure within 90 days of receipt of the report.
4. The complaint shall be declared inadmissible if the complainant has brought an action before the judicial authority.

Art.68
(Reporting)

1. Anyone may report to the Data Protection Authority if they believe there are any infringements of this Law.
2. The Data Protection Authority shall handle the report by its own measure:

Art.69
(Objection)

1. Against the measure issued by the Data Protection Authority, including the administrative fines referred to in Articles 72 and 73, the controller or the data subject may lodge an objection by a judicial appeal in accordance with Article 70. The objection shall not suspend the enforcement of the relevant measure.
2. The Judicial Authority shall act in accordance with Article 70.

Art.70
(Judicial protection)

1. All disputes concerning the application of the provisions of this Law shall be assigned to the ordinary judicial authority.
2. Without prejudice to Article 69, natural or legal persons shall have the right to lodge a judicial appeal against a legally binding decision of the Data Protection Authority concerning them.
3. Every data subject shall have the right to lodge a judicial appeal if the Data Protection Authority does not handle a report or a complaint.
4. Without prejudice to the right to lodge a complaint with the Data Protection Authority, data subjects shall have the right to lodge a judicial appeal with the ordinary judicial authority if they consider that their rights they enjoy pursuant to this Law have been infringed as a result of the processing by a controller or processor established in the Republic of San Marino.

Art. 71
(Right to compensation and liability)

1. Any person who has suffered material or non-material damage as a result of an infringement of this Law shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the ordinary judicial authority.

TITLE VIII
ADMINISTRATIVE FINES

Art.72
(Infringements committed by the controller or processor)

1. Infringements of the following provisions shall be subject to administrative fines up to five million euros (5,000,000.00 EUR), or in the case of an undertaking, up to 2 % of the total annual turnover of the previous financial year, whichever is higher:
a) the obligations of the controller and the processor pursuant to Articles 7, 11, 24 to 40, 43 and 44;
b) the obligations of the certification body pursuant to Articles 43 and 44;
c) the obligations of the monitoring body in accordance with Article 42.

2) Infringements of the following provisions shall be subject to administrative fines up to ten million euros (10,000,000.00 EUR), or for undertakings, up to 4 % of the total annual turnover in the preceding financial year, whichever is higher:
a) the basic principles of processing, including conditions for consent, pursuant to Articles 4, 5, 6 and 8;
b) the data subjects' rights pursuant to Articles 12 to 22;
c) the transfers of personal data to a recipient in a foreign country or an international organisation pursuant to Title V of this Section;
d) non-compliance with an order, a temporary or definitive limitation on processing or the suspension of data flows by the Data Protection Authority pursuant to Article 59, paragraph 2, or failure to provide access in violation of Article 59, paragraph 1.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. The provisions contained in this Article may be amended by a delegated decree.

Art.73
(Procedures for imposing fines)

1. The Data Protection Authority shall be the competent body to receive the report and to impose fines referred to in this Chapter.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 59, paragraph 2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
b) the intentional or negligent character of the infringement;
c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;
e) any relevant previous infringements by the controller or processor;
f) the degree of cooperation with the Data Protection Authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g) the categories of personal data affected by the infringement;
h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
i) where measures referred to in Article 59, paragraph 2 have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
l) adherence to approved codes of conduct pursuant to Article 41 or approved certification mechanisms pursuant to Article 43; and
m) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
3. The Data Protection Authority shall ensure that the administrative fines imposed are in any case effective and proportionate.

PART II
SPECIFIC PROVISIONS FOR THE PROCESSING OF PERSONAL DATA FOR COMPLIANCE WITH A LEGAL OBLIGATION, FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR IN THE EXERCISE OF OFFICIAL AUTHORITY

TITLE I
PROVISIONS ON THE LEGAL BASIS

Art.74
(Legal basis)

1. The provisions contained in this Section shall be established for implementing the provisions of Article 5, paragraph 1, letter c) and e).
2. In addition, rules shall be laid down limiting the scope of the obligations and the rights referred to in Articles 12 to 22, in order to safeguard the independence of the judiciary and judicial proceedings.
3. Processing operations carried out for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as referred to in Article 5, paragraph 1, letter e) of this Law, shall not be subject to the right provided for in Articles 17 and 20 of this Law.

TITLE II
PROCESSING IN THE JUDICIAL SECTOR

Art.75
(News or images related to children)

1. The publication and dissemination, by any means, of news or images suitable for identifying a child involved, for whatever reason, in legal proceedings, shall be prohibited.
2. Any infringement of the prohibition set out in this Article shall be punished pursuant to Article 192 bis of the Criminal Code.

Art. 76
(Civil and administrative judgements and judicial orders)

1. Judgements and other judicial orders issued by the civil and administrative judicial authority of any level and instance shall be published in full. However, in the copies thereof, personal data of the parties shall be made anonymous in advance, by indicating only initials of the name and, if the personal data concern children, any identification data relating to them shall be made anonymous.
2. In other cases, they may be anonymised only with the prior authorisation of the competent magistrate who may evaluate the request of the party concerned, to be deposited at the competent Registry during the proceedings and in any case before the issue of the first instance's judgement.
3. Copies of decrees concerning non-contentious proceedings shall never be anonymised, except in the area of child protection, unless they concern authorisation to draw up public acts or acts in favour of the child, for which anonymisation would be prejudicial.
4. In the cases referred to in the first paragraph and of judicial authorisation for the anonymisation of the judgement or order, the Registrar may issue only anonymised certified copies unless a reasoned request is submitted in the interests of the parties or their guardians or successors in title, on which the competent judge shall decide.
5. Judgements and other decisions of the judicial authorities of any level and instance deposited at the Registry shall be made available to those who have an interest therein and may be published in the press, on institutional and/or informational websites for the purposes of studies and for the gathering of case law.
6. Where such judgements and order concern children or have been made anonymous, they may only be made accessible by mentioning they have been anonymised and only as such may they be published in the press or on websites.
7. Copies of anonymised judgements may be sent by the Registry in full if they are transmitted to the public administration offices, which shall use them for official purposes, taking care that they are not disclosed in full.

76-bis
(Criminal judgements and judicial orders)

1. Judicial orders and criminal judgements of any level and instance shall be issued and published according to the rules provided by criminal laws and criminal procedure in force in the Republic of San Marino. The Register of criminal convictions shall only be kept by the public authority that may issue certificates where convictions are recorded.
2. Copies of criminal judgements shall be anonymised ex-officio by the Registry at the end of the document only if they concern children or if such anonymisation is necessary to avoid the

identification of a child who is a civil party or an injured party, as well as in all cases where proceedings are held in camera, to protect the identity of the victim.
3. Copies of anonymised judgements may be sent by the Registry in full if they are transmitted to the public administration offices, which shall use them for official purposes, taking care that they are not disclosed in full.

TITLE III
STATE DEFENCE AND SECURITY

Art.77
(Processing of personal data for national security or defence purposes)

1. The provisions of this Law shall apply to the processing of personal data covered by State secrecy or data covered by State secrecy, only to the extent provided for in Article 63.
2. Without prejudice to the provisions of paragraph 1, the provisions of this Law shall apply to the processing carried out by public entities for State defence or security purposes, on the basis of explicit legal provisions that specifically provide for the processing, only to the extent referred to in paragraph 1.
3. A specific delegated decree shall identify the methods of application of the provisions referred to in paragraph 1 with regard to the types of data, data subjects, processing operations that can be performed and persons authorized to process personal data under the direct authority of the controller or the processor or expressly designated pursuant to Article 30, including in relation to updating and storage.

TITLE IV
PROCESSING OF PERSONAL DATA IN THE HEALTH SECTOR

Art.78
(Processing of personal data in the health sector)

1. Entities and bodies, including private ones, which are part of the health system of the Republic of San Marino shall process personal data and in particular data concerning health only on the basis of this Law.
2. The right referred to in Articles 17 and 20 of this Law shall not apply to the processing of personal data for the purpose of protecting the health and physical safety of the data subject or third parties or the community.

Art.79
(Transparency of the processing of personal data by entities and bodies forming part of the health system of the Republic of San Marino)

1. The entities and bodies, including private ones, which are part of the health system of the Republic of San Marino shall process personal data and in particular data concerning health and shall provide the data subjects beforehand with the information laid down in Articles 13 and 14, analytically highlighting any processing of personal data presenting specific risks to the fundamental rights, freedoms and dignity of the data subject, in particular where such processing:
a) concerns genetic data;
b) is carried out for scientific purposes, including scientific research and controlled clinical trials of medicinal products, in accordance with current regulations, with particular emphasis on the fact that consent, where required, is freely given;
c) uses automated data processing systems, including in the field of teleassistance or telemedicine;
d) is carried out in order to provide other goods or services to the data subject via an electronic communications network.

Art.80
(Lawfulness of personal data processing by health entities and bodies)

1. The entities and bodies, including private ones, which are part of the health system of the Republic of San Marino shall process personal data and in particular data concerning health for their official aims, even in the context of an activity of substantial public interest, when data subjects have given explicit consent to the processing of those personal data for one or more specified purposes of protecting their health or physical safety.
2. Personal data and in particular data concerning health shall also be processed without consent in the event that:
a) processing is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent or it is necessary to protect the vital interest of a third party or the community;
b) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of current law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
c) processing is necessary for reasons of substantial public interest, and shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
d) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of San Marino law.

Art.81
(Measures to respect the rights of data subjects)

1. The entities and bodies, including private ones, which are part of the health system of the Republic of San Marino shall take proper measures to ensure, in the provision of services, the respect of rights, fundamental freedoms and dignity of the data subjects, without prejudice to what is further provided for by the law in force on the provision of health services and the respective structural and organizational requirements.
2. The measures referred to in paragraph 1, adopted after a specific risk assessment subject to periodic and documented reassessment, shall also include:
a) solutions aimed at respecting an order of precedence and call of the subjects without being identified by name in relation to health services or administrative requirements while waiting within the facilities;
b) possible use of acoustic equipment or barriers, other devices or solutions to keep distance and ensure confidentiality in the interaction between healthcare professionals and patients to prevent the undue knowledge by third parties of information likely to reveal the state of health;
c) precautions to ensure that health services, including any medical history documents, are not provided in situations where other people are present by reason of the methods or premises chosen;
d) anything necessary to ensure that, when medical services are provided and in all data processing operations, respect for the dignity of the data subject is guaranteed.

Art.82
(Disclosure of personal data)

1. Entities and bodies, including private ones, that are part of the health system of the Republic of San Marino shall take the necessary measures to ensure that:
a) personal data revealing the state of health may be disclosed to the data subjects and their delegates only by health staff specifically delegated for this purpose;
b) the correct notification or confirmation, including by telephone, of a first aid service shall be given only to legitimate third parties;
c) proper procedures shall be adopted to disclose to legitimate third parties, in accordance with the internal regulations of the hospital and territorial facilities, the presence and location at these facilities of the data subjects, respecting any contrary will;
d) staff and collaborators who process personal data are subject to compulsory and continuous training, aimed at preventing with regard to strangers, in particular, an explicit correlation between the data subject and wards or facilities or indicating the existence of a specific state of health.

Art.83
(Documents)

1. In cases where entities and bodies, including private ones, that are part of the health system of the Republic of San Marino draw up and keep medical records or other health documents, proper measures shall be taken to distinguish the data relating to the patient from those that may concern other data subjects.
2. Any requests for access shall be processed in the light of the provisions of Article 30 of Law no. 160 of 5 October 2011 and subsequent amendments and integrations.

TITLE V
OTHER PUBLIC PROCESSING OPERATIONS OR OF PUBLIC INTEREST

Chapter I INSURANCES

Art.84
(Accidents)

1. The Central Bank of the Republic of San Marino shall establish by its own decree the procedures and methods of operation of the accident database created for the prevention and combating of fraudulent behaviour in the compulsory insurance sector for motor vehicles registered in the Republic of San Marino, the procedures for the access to the information collected in the database by the judicial bodies and for the public administrations competent for the prevention and combating of fraudulent behaviour in the compulsory insurance sector, as well as the procedures and limits for access to information by insurance undertakings.
2. The processing and disclosure of personal data to the data subjects referred to in paragraph 1 shall be permitted for the performance of the functions indicated in the same paragraph.

CHAPTER II
EDUCATION AND TRAINING

Art.85
(Special categories of personal data)

1. In accordance with Article 8, paragraph 2, letter g), the purposes of education and training in school, professional education, higher education or university, with particular reference to those carried out also in an integrated form, shall be considered to be of significant public interest.

Art.86
(Processing of data relating to students)

1. In order to facilitate guidance, training and professional integration, including abroad, schools and secondary schools may, at the request of data subjects, disclose or disseminate, including to private individuals and by electronic means, data, both intermediate and final, on school results of the students and other personal data other than those referred to in Articles 8 and 10, relevant in relation to the aforesaid purposes and indicated in the information provided to the data subjects pursuant to Article 13. The data may subsequently be processed exclusively for the aforementioned purposes.
2. The student's right to confidentiality shall remain unaffected. The provisions in force concerning the publication of the results of examinations by posting them in the institute register and the issue of diplomas and certificates shall also remain unaffected.

PART III
PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

TITLE I
JOURNALISM, FREEDOM OF INFORMATION AND OF EXPRESSION

Art.87
(Journalistic purposes and other expressions of thought)

1. The provisions of this Title shall apply to processing operations:
a) carried out in the exercise of the profession of journalist and for the exclusive pursuit of its objectives;
b) carried out by persons registered in the register kept by the Council for Information referred to in Article 5 of Law no. 211 of 5 December 2014 and subsequent amendments and integrations;
c) aimed exclusively at the publication or occasional dissemination of articles, essays and other expressions of thought, including of an academic, artistic and literary nature.

Art.88
(Applicable provisions)

1. With reference to the provisions of Article 87, the data referred to in Articles 8 and 10 of this Law may be processed without the consent of the data subject, provided that the provisions of the code of conduct referred to in Article 90 are complied with.
2. The provisions of Article 9 and Title V of Part I concerning the transfer of data abroad shall not apply to the processing operations referred to in Article 87.
3. In the case of dissemination or disclosure of data for the purposes referred to in Article 87, the limits to press freedom for the protection of the rights referred to in Articles 1 and 5, in particular the essential nature of the information on facts in the public interest, shall not be affected. Personal data relating to circumstances or facts disclosed directly by the data subjects or through their behaviour in public may be processed.

Art.89
(Professional secrecy)

1. If the data subject requests to be informed of the source of the personal data pursuant to Article 15, paragraph 1, letter g), the rules on the professional secrecy of journalists, limited to the source of the information, shall remain unaffected.

Art.90
(Code of conduct for journalistic activities)

1. The Data Protection Authority shall promote, in accordance with Article 41, the adoption by the Council for Information, referred to in Article 5 of Law no. 211 of 2014 and subsequent amendments and integrations, of a code of conduct on the processing of data referred to in Article 87, which provides for measures and mechanisms to protect the data subjects in relation to the nature of the data, particularly with regard to those concerning health and life or sexual orientation. The code may also provide for simplified forms for the information referred to in Articles 13 and 14.
2. The adoption of the code of conduct shall take place within twelve months from the date of entry into force of this Law.
3. In the period between the date of entry into force of this Law and the adoption of the code of conduct, or subsequently, the Data Protection Authority, in cooperation with the Council for Information, shall establish any measures and mechanisms to guarantee the data subjects, which the Council shall be required to transpose.
4. The code or the amendments or integrations to the code of conduct which are not adopted by the Council within six months of the proposal of the Data Protection Authority, shall be adopted by the Data Protection Authority and shall be effective until the latter and the Council for Information have established a different discipline, according to the procedure of cooperation referred to in

paragraph 2.
5. In case of infringements of the provisions contained in the code of conduct, the Data Protection Authority may prohibit the processing.

TITLE II
ACCESS TO ADMINISTRATIVE DOCUMENTS

Chapter I ACCESS

Art.91
(Access to administrative documents)

1. The conditions, procedures and limits to exercise the right of access to administrative documents containing personal data, and the relative judicial protection, shall remain governed by Law 160 of 5 October 2011 and subsequent amendments, also with regard to the particular categories of personal data and personal data relating to criminal convictions and criminal offences, as well as the processing operations that can be carried out in execution of a request for access.
2. In line with the provisions of article 5 of Law no. 159 of 5 October 2011 and article 19 of Law no. 160 of 5 October 2011, the data acquired by organisational units (OU) of the Public Administration, by organisational structures of Autonomous State Corporations and Public Bodies and by providers of public services in the exercise of their functions, shall be legitimately processed for the performance of tasks of public interest or connected with the exercise of public powers, by any other OU and organisational structure of the Overall Public Sector and operator of a public service, without the need for the consent by the data subject.
3. In any case, the provisions of Article 5, paragraph 4, letter d) of Law no. 159 of 2011 shall remain unaffected for the providers of public services.
4. The provision of paragraph 2 shall also apply to personal data collected and stored in the Criminal Records.
5. The provision of paragraph 2 shall not apply to the data referred to in Article 8, paragraph 1.

Chapter II
PUBLIC AND PROFESSIONAL REGISTERS

Art.92
(Use of public data)

1. The Data Protection Authority shall promote the drawing up of a code of conduct for the processing of personal data from archives, registers, lists, deeds or documents kept by public bodies, also identifying the cases in which the source of data shall be indicated and providing proper guarantees for the association of data from more than one archive.
2. For the purposes of this Law, personal data other than special categories of personal data or personal data relating to criminal convictions and criminal offences, which shall be included in a professional register in accordance with the law or a regulation, may be disclosed to public and private entities or disseminated also by electronic communications networks. The existence of measures ordering suspension or affecting the exercise of the profession may also be mentioned.
3. The professional association may, at the request of the person registered in the register that has an interest in it, supplement the data referred to in paragraph 2 with additional relevant data and not exceeding the boundaries of professional activity.
4. At the request of the data subject, the professional association may also provide third parties with information relating, in particular, to special professional qualifications not mentioned in the register, or to the willingness to take on assignments or to receive information material of a scientific nature also relating to conferences or seminars.

TITLE III
PROCESSING IN THE CONTEXT OF THE EMPLOYMENT RELATIONSHIP

CHAPTER I
GENERAL PROFILES

Art.93
(Employment guarantee measures)

1. Pursuant to Article 8, paragraph 2, letter b), the Data Protection Authority may adopt measures and mechanisms, also in relation to certain categories of controllers or processing operations, in order to identify specific guarantees for the processing of personal data carried out in the context of employment relationships. Such measures shall include proper and specific measures to safeguard human dignity, legitimate interests and fundamental rights of the data subjects, in particular with regard to the purpose of recruitment, execution of the employment contract, including fulfilment of obligations laid down by Law or by collective agreements, management, planning and work organisation, equality and diversity at work, and health and safety at work, protection of the property of the employer or the client and for the purpose of exercising and enjoying, individually or collectively, rights and benefits linked to employment, for the purpose of terminating the employment relationship, as well as the transparency of processing, the transfer of personal data within an entrepreneurial group or a group of undertakings carrying out a joint activity and monitoring systems in the workplace.

Art.94
(Code of conduct)

1. The Data Protection Authority shall promote the adoption of a code of conduct for public and private subjects involved in the processing of personal data carried out within the framework of the employment relationship for the purposes referred to in Article 93, also providing specific procedures for the information to be returned to the data subject.

Art.95
(Information in case of receipt of curriculum vitae)

1. The information referred to in Article 13 and consent to processing shall not be given in the event of receipt of curriculum vitae spontaneously transmitted by the data subjects for the purposes of any establishment of an employment relationship. The information shall however be provided at the time of the first contact following the sending of the curriculum.

CHAPTER II
PROCESSING OF DATA RELATING TO EMPLOYEES

Art.96
(Data collection and relevance)

1. The provisions of Article 14 of Law No. 95 of 19 September 1989 and subsequent amendments and integrations shall remain unaffected.
2. At the time of hiring, the employer shall provide the data subject with the information required by this Law.

Art.97
(Domestic employment relationship)

1. In the context of the domestic work relationship, the employer shall be required to ensure that the worker's personality and self-determination are respected.
2. The domestic worker shall be required to maintain the necessary confidentiality for all matters relating to family life.

TITLE IV
PROCESSING OF PERSONAL DATA FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH OR FOR STATISTICAL PURPOSES

CHAPTER I
GENERAL PROVISIONS

Art.98
(Scope of application)

1. This Title shall regulate the processing of personal data for archiving purposes in the public interest, scientific or historical research or for statistical purposes.
2. Without prejudice to the provisions of this Title, processing for archiving purposes in the public interest, scientific or historical research or for statistical purposes shall be subject to appropriate safeguards for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
3. The rules set out in Law no. 50 of 11 May 2012 shall apply.

Art.99
(Duration of the processing)

1. The processing of personal data for archiving purposes in the public interest, scientific or historical research or for statistical purposes may be carried out also beyond the period of time necessary to achieve the various purposes for which the data were previously collected or processed.
2. For archiving purposes in the public interest, scientific or historical research or for statistical purposes, those personal data the processing of which has ceased for any reason may in any case be stored or transferred to another controller.

Art.100
(Data concerning studies and research)

1. In order to promote and support research and collaboration in the field of science and technology, public entities, including research institutions may, by their own decision, communicate or disseminate, including to individuals and electronically, data relating to studies and research, graduates, PhDs, technicians and technologists, researchers, teachers, experts and scholars, with the exception of special categories of personal data and personal data relating to criminal convictions and crimes.
2. The right of the data subject to rectification, erasure and objection pursuant to Articles 16, 17 and 21 shall remain unaffected.
3. The data referred to in this article shall not constitute administrative documents in accordance with Law 160 of 5 October 2011 and subsequent amendments.
4. The data referred to in this article may subsequently be processed only for the purposes on the basis of which they are communicated or disseminated.
5. The rights referred to in paragraph 2 shall be exercised in accordance with the procedures laid down in the Codes of Conduct.

Chapter II
PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST OR HISTORICAL RESEARCH PURPOSES

Art.101
(Processing procedures)

1. Personal data collected for archiving purposes in the public interest or historical research may not be used to adopt acts or administrative measures unfavourable to the data subject, unless they are used for other purposes in compliance with Article 4 of this Law.
2. Documents containing personal data, processed for archiving purposes in the public interest or historical research purposes, may be used, taking into account their nature, only if relevant and indispensable to the pursuit of such purposes. Personal data disseminated may be used only for the pursuit of the same purposes.
3. Personal data may in any case be disseminated when they relate to circumstances or facts

made known directly by the data subject or through his conduct in public.

Art.102
(Code of conduct)

1. The Data Protection Authority shall promote, pursuant to Article 41, the drawing up of a code of conduct for public and private entities, including scientific undertakings and professional associations, interested in the processing of data for archiving purposes in the public interest or historical research purposes.
2. The code of conduct referred to in paragraph 1 shall identify, in particular:
a) the rules of fairness and non-discrimination towards users, to be observed also in the communication and dissemination of data, in accordance with the provisions of this Law applicable to data processing for journalistic purposes or the publication of articles, essays and other expressions of thought including in artistic expression;
b) special precautions for the collection, consultation and dissemination of documents concerning data revealing health status, sex life or confidential family relationships, identifying cases in which the data subject or those interested therein are informed by the user of the intended dissemination of data;
c) the procedures for applying to private archives the rules governing the processing of data for archiving purposes in the public interest or historical research purposes, also with reference to the uniformity of the criteria to be followed for consultation and the precautions to be observed in communication and dissemination.

Art.103
(Consultation of documents kept in archives)

1. Consultation of documents kept in the archives forming part of the documentary and archival heritage of the Republic shall be governed by Law no. 50 of 11 May 2012.

CHAPTER III
PROCESSING FOR STATISTICAL PURPOSES OR FOR SCIENTIFIC RESEARCH PURPOSES

Art.104
(Scope of application and identification data for statistical or scientific purposes)

1. The provisions of this Chapter shall apply to the processing of data for statistical purposes or, as far as compatible, for scientific research purposes.
2. To implement the provisions of this Chapter, with regard to identification data, account shall be taken of all the means which may reasonably be used by the controller or by other parties to identify the data subject, including on the basis of knowledge acquired in relation to technical progress.

Art.105
(Processing procedures)

1. Personal data processed for statistical or scientific purposes may not be used for taking decisions or measures with regard to the data subject, nor for processing data for other purposes.
2. The statistical or scientific purposes shall be clearly determined and made known to the data subject, following the procedures referred to Articles 13 and 14, including in relation to the provisions of Article 106, paragraph 2, letter b).
3. Where specific circumstances identified by the codes referred to in Article 106 are such as to enable a person to respond in the name and on behalf of another, either as a family member or as a cohabiting partner, information may also be given to the data subject through the respondent.
4. For the processing carried out for statistical or scientific purposes in relation to data collected for other purposes, information shall be provided to the data subject only when such provision involves a proportionate effort in relation to the protected right, after proper forms of publicity specified in the codes referred to in Article 106 have been adopted.

Art.106
(Codes of conduct)

1. Pursuant to Article 41, the Data Protection Authority shall promote the drawing up of one or more codes of conduct for public and private entities, including scientific undertakings and professional associations, interested in the processing of data for statistical or scientific purposes.
2. The codes referred to in paragraph 1 shall identify:
a) the conditions and procedures to document and verify that processing is carried out for suitable and effective statistical or scientific purposes;
b) for what is not foreseen by this Law, the further conditions of processing and the connected safeguards, also with reference to the duration of data storage, the information to be given to the data subjects on the data collected also at third parties' premises, the communication and dissemination, the selective criteria to be met for the processing of identification data, the specific security measures and the procedures to modify the data following the exercise of the rights of the data subject;
c) all the means likely to be reasonably used by the controller or by other parties to identify the data subject, including in relation to knowledge acquired as a result of technical progress;
d) the safeguards to be granted to apply the provisions allowing the consent of the subject to be disregarded;
e) simplified procedures for the data subjects to give their consent to the processing of special categories of personal data;
f) the cases when the rights referred to in Articles 15, 16, 18 and 21 may be restricted;
g) the rules of fairness to observe in data collection and the instructions to be given to persons authorised to process personal data under the direct authority of the controller or processor or expressly designated in accordance with Article 30;
h) the measures to be adopted to promote compliance with the principle of minimisation and with the technical and organisational measures referred to in Article 33, including with reference to the precautions aimed at preventing access by natural persons who are not authorised or designated and the unauthorised identification of data subjects, the interconnection of information systems also within the scope of the IT, Technology, Data and Statistics Office and the exchange of data for statistical or scientific purposes to be carried out with bodies and offices located abroad;
i) the commitment to comply with the rules of conduct of persons authorised to process personal data under the direct authority of the controller or processor, who are not bound by law to professional secrecy, which ensure similar levels of security and confidentiality.

Art.107
(Processing of special categories of personal data)

1. Without prejudice to the provisions of Article 8 and except for the cases of specific statistical surveys or scientific research provided for by the law, the consent of the data subject to the processing of specific categories of personal data, when requested, may be given in a simplified manner, as specified by the code referred to in Article 106.

Art.108
(Medical, biomedical and epidemiological research)

1. The consent of the data subject to the processing of health data for scientific research purposes in the medical, biomedical or epidemiological fields shall not be necessary when the research is conducted in compliance with the legal provisions referred to in Article 8, paragraph 2, letter j), of this Law, and an impact assessment is conducted and made public pursuant to Articles 36 and 37 of this Law. The consent shall also not be required when, because of specific reasons, informing the data subjects is impossible or involves a disproportionate effort, or is likely to render impossible or seriously impair the achievements of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject; the research programme shall be the subject of a reasoned opinion by the San Marino Bioethics Committee (SMBC) referred to in Law no. 34 of 29 January 2010 and its Delegated Decree no. 2 of 17 January 2011, and shall be authorised by the Data Protection Authority or subject to its prior consultation pursuant to Article 37 of this Law.
2. When the data subjects exercise the rights pursuant to article 16 of this Law with regard to

the processing operations referred to in paragraph 1, the rectification and integration of the data shall be recorded without changing them, when the result of such operations does not have a significant effect on the result of the research.

Art.109
(Re-use of data for scientific research or statistical purposes)

1. The Data Protection Authority may authorise the re-use of data, including those relating to the processing of particular categories of personal data, with the exception of genetic data, for the purposes of scientific research or for statistical purposes by persons who carry out mainly such activities when, because of particular reasons, informing the data subjects is impossible or involves a disproportionate effort, or is likely to render impossible or seriously impair the achievement of research purposes, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subject, including preventive forms of data minimisation and pseudonymisation.
2. The Data Protection Authority shall communicate the decision adopted on the request for authorization within sixty days, after which failure to respond shall be equivalent to a rejection. By its decision on the authorization or even later, on the basis of any checks, the Data Protection Authority shall establish the conditions and measures necessary to ensure proper safeguards for the protection of data subjects in the context of data re-use, including from the point of view of their security.

SECTION IV
ELECTRONIC COMMUNICATION

Art.110
(Services concerned)

1. The provisions of this Section IV shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services on public communications networks, including those using data collection and identification devices.

Art.111
(Information collected about the subscriber or the user)

1. The storage of information on the terminal equipment of a subscriber or user or access to information already stored shall be permitted only if subscribers or users have given their consent after having been informed in accordance with Articles 13 and 14. This shall not preclude any technical storage of or access to already stored information for the sole purpose to transmit a communication on an electronic communications network, or to the extent strictly necessary for the provider of an information communication service explicitly requested by the subscriber or user to provide such a service. To determine the above mentioned simplified procedures, the Data Protection Authority shall also take into account the proposals made by the most representative consumer associations and economic categories involved at national level, to also guarantee the use of procedures that ensure effective awareness of subscribers or users.
2. To give the consent referred to in paragraph 1, specific configurations of computer software or devices may be used as long as they are easy and clear for subscribers or users.
3. Without prejudice to paragraph 1, the use of an electronic communications network to access information stored in the terminal equipment of a subscriber or a user, to store information or to monitor user operations shall be prohibited.

Art.112
(Traffic data)

1. Traffic data relating to subscribers and users processed by the provider of a public telecommunications network or publicly available electronic telecommunications services shall be erased or made anonymous when they are no longer required for the transmission of electronic communication, without prejudice to the provisions of paragraphs 2, 3 and 5.
2. The processing of traffic data strictly necessary for billing purposes for the subscriber, or

payments in the event of interconnection, shall be allowed to the provider, for documentation purposes, in the event of a dispute over billing or payments, for a period not exceeding six months, without prejudice to the further specific storage required as a result of a dispute, including in court.

3. The provider of a publicly available electronic communications service may process the data referred to in paragraph 2 to the extent and for the duration necessary for the purpose of marketing electronic telecommunications services or for the provision of value-added services only if the subscriber or user to whom the data relate has given his prior consent, which may be withdrawn at any time.

4. In providing the information referred to in Articles 13 and 14, the service provider shall inform the subscriber or user of the nature of the traffic data that are processed and of the duration of such processing operation for the purposes referred to in paragraphs 2 and 3.

5. Processing of traffic data must be restricted to processors acting under the authority of providers of the public telecommunications networks or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services or provision of value-added services. Processing shall be restricted to what is strictly necessary to carry out such activities and shall ensure the identification of the person acceding personal data, even by means of an automated search procedure.

Art.113

(Itemized billing)

1. Subscribers shall have the right to receive, upon request and free of charge, itemised bills with proof of the elements that make up the bill relating, in particular, to the date and starting time of the conversation, the dialled number, the type of numbering, the location, the duration of the calls and the number of units to be charged for each conversation.

2. Providers of publicly available electronic communications services shall be required to enable users to communicate and request services from any terminal, free of charge and via a simple means, using alternative modalities to billing for payments, even impersonal, such as credit or debit cards or prepaid cards.

3. The documentation sent to subscribers relating to the communications made shall not contain the services and communications referred to in paragraph 2, nor the communications necessary to activate the alternative modalities to billing

4. The last three digits of the numbers called shall not be reported in the subscribers' bills. For the sole purpose of challenging the correctness of the fees charged or related to limited periods, subscribers may request the communication of the full numbers of the relevant telephone calls.

5. The Data Protection Authority, after having ascertained the effective availability of the modalities referred to in paragraph 2, may authorize the provider to indicate in the bills the full numbers of the telephone calls.

Art. 114

(Calling line identification)

1. Where presentation of calling-line identification is offered, the provider of the publicly available electronic communications service shall provide the calling user with the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling-line identification is offered, the provider of the publicly available electronic communications service shall provide the calling user with the possibility via a simple means, free of charge, to prevent the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the provider of the publicly available electronic communications service shall provide the called subscriber with the possibility via a simple means, free of charge, to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the provider of the publicly available electronic communications service shall provide the called subscriber with the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification

to the calling user.
5. The provisions set out in paragraph 1 shall also apply with regard to calls to foreign countries. The provisions set out in paragraphs 2, 3 and 4 shall also apply to incoming calls originating in such countries.
6. Where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services shall inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Art.115
(Location data)

1. Location data other than traffic data relating to users or subscribers of public communications networks or publicly available electronic communications services may be processed only if they are made anonymous or with the consent of the user or subscriber concerned, which may be withdrawn at any time, to the extent and for the duration necessary for the provision of a value-added service.
2. The service provider, before obtaining their consent, shall inform users and subscribers of the type of location data other than traffic data that will be processed, the purposes and duration of the processing and whether the data will be transmitted to a third party for the provision of a value-added service.
3. Users and subscribers having given their consent to the processing of location data other than traffic data, shall preserve the right to request, free of charge and via a simple means, a temporary interruption of the processing of such data for each connection to the network or for each transmission of communications.
4. Processing of location data other than traffic data under paragraphs 1, 2 and 3 shall only be allowed to persons in charge of the processing acting under the authority of the provider of the publicly available electronic communications service or, as applicable, of the provider of the public communications network or of the third party providing the value-added service. Processing shall be restricted to that which is strictly necessary for the provision of a value-added service and shall ensure the identification of the person acceding personal data, even by means of an automated search procedure.

Art.116
(Disturbing and emergency calls)

1. Subscribers receiving disturbing calls may request that the provider of the public communications network or publicly available electronic communications service override the elimination of the presentation of calling line identification and store the data containing the origin of the call received on a temporary basis. The elimination of the presentation of the calling line may be overridden only for the periods of time during which disturbing calls occur and for a period not exceeding fifteen days.
2. The written request of a subscriber shall describe the way disturbing calls were received and, if preceded by a telephone request, shall be made within 48 hours.
3. The data stored in accordance with paragraph 1 may be communicated to the subscriber stating that he uses them for exclusive purposes of protection against disturbing calls. For the services referred to in paragraph 1, providers shall ensure transparent procedures vis-à-vis subscribers and may charge a fee which shall not exceed the actual costs incurred.
4. The provider of a public communications network or publicly available electronic communications service shall establish transparent procedures to ensure, on a per-line basis, the elimination of the presentation of calling line identification and, where necessary, the processing of location data, notwithstanding the temporary refusal or absence of consent of the subscriber or user, by lawfully authorised services to receive emergency calls.

Art. 117
(Automatic call forwarding)

1. The provider of a publicly available electronic communications service shall take the necessary measures to ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

Art. 118
(Directories of subscribers)

1. The Data Protection Authority shall identify by its own measure how to enter and use personal data relating to subscribers in printed or electronic directories of subscribers available to the public.
2. The measure referred to in paragraph 1 shall identify suitable methods for subscribers to give their consent to the publication of personal data in the directories and to indicate that their personal data may be used for the purposes referred to in paragraph 1, letter c) and 21, paragraph 2, based on the principle of maximum simplification of the methods of inclusion in the directories for pure purposes of subscribers tracing for interpersonal communications, and specific and express consent when the processing is not in line with such purposes, as well as consent on the verification, rectification or erasure of data free of charge.

Art. 119
(Unsolicited communications)

1. The use of automated calling or communication systems without human intervention for the purposes of direct marketing, direct selling, market research or business communication may only be allowed in respect of subscribers or users who have given their prior consent.
2. The provision referred to in paragraph 1 shall also apply to electronic communications, carried out for the purposes indicated therein, by e-mail, fax, messages such as MMS (Multimedia Messaging Service) or Sms (Short Message Service) or other types.
3. Except for the cases referred to in paragraphs 1 and 2, further communications for the purposes referred to in the same paragraphs, carried out by means other than those indicated therein, shall be allowed pursuant to Articles 5 and 6 and paragraph 4 of this Article.
4. By way of derogation from Article 118, processing of the data referred to in Article 118, paragraph 1, through the use of telephone and paper mail for the purposes of direct marketing, direct selling, market research or business communication shall be allowed in respect of those who have not exercised their right to object, in simplified ways and also electronically, by indicating their phone numbers and other personal data referred to in Article 118, paragraph 1, in a public objections register.
5. The register referred to in paragraph 4 shall be established by delegated decree according to the following criteria and general principles:
a) the establishment and management of the register shall be entrusted to a public body or entity with competence in the field;
b) the entity or body responsible for establishing and managing the register shall do so with the human and instrumental resources at its disposal or by entrusting its implementation and management to third parties, who shall bear the entire financial and organisational costs, by means of a service contract, in compliance with the rules on public contracts relating to works, services and supplies. The entities using the register to send communications shall pay access fees based on actual operating and maintenance costs. The Congress of State, by its own measure, shall determine such fees;
c) the technical methods of operation of the register shall allow users to request that their telephone number be registered in a simplified manner, including electronically or by phone;
d) the technical methods of operation and access to the register by selective questions shall not allow the transfer of data entered in the register; however such methods shall allow the tracking of access and processing operations through retention of logs;
e) provisions shall be issued relating to the timing and methods of entering in the register shall be regulated, irrespective of the area of activity or product category, the updating of the registration, as well as the maximum period of usability of the data verified in the register; based on such provisions, the registration shall be for an indefinite period and may be revoked at any time, through user-friendly instruments and free of charge;
f) the entities processing data for the purposes of direct marketing, direct selling, market research or business communication shall ensure the presentation of the calling line identification and provide users with appropriate information, in particular on the possibility and methods of registration to object future contacts;
g) entering in the register shall not preclude the processing of data otherwise obtained and processed in accordance with Articles 5 and 6.

6. Supervision and control over the organisation and functioning of the register referred to in paragraph 4 and over the processing of data shall be assigned to the Data Protection Authority.
7. Without prejudice to the provisions of paragraph 1, if the data controller uses, for the purposes of direct selling of its products or services, the e-mail address provided by the data subject in the context of a sale of a product or service, the controller may not require the consent of the data subject, provided that these services are similar to those being sold and the data subject, appropriately informed, does not refuse such use, initially or in subsequent communications. The data subject shall be informed, at the time of collection and on the occasion of each communication for the purposes referred to in this paragraph, of the possibility of objecting at any time to the processing, easily and free of charge.
8. In any event, the practice of sending communications for the purposes referred to in paragraph 1 or for promotional purposes which disguise or conceal the identity of the sender, or which do not have a valid address to which the recipient may exercise the rights referred to in Articles 15 to 22 or which encourage recipients to visit websites that contravene Article 28 of Law no. 58 of 29 May 2013 shall be prohibited.
9. In case of a repeated breach of the provisions referred to in this Article, the Data Protection Authority may also require providers of electronic communications services to adopt filtering procedures or other practicable measures regarding the e-mail address from which communications were sent, pursuant to Article 59.

Art.120
(Information to subscribers and users)

1. The provider of a publicly available electronic communications service shall be obliged to inform the subscriber and, where possible, the user of the existence of situations which make it possible to learn unintentionally the content of communications or conversations by persons who are not parties thereto.
2. The subscriber shall inform the user when the content of the communications or conversations may be learned by others due to the type of terminal equipment used or the connection made between them at the subscriber's premises.
3. The user shall be required to inform the other user when, during the conversation, devices are used that allow other parties to listen to the conversation.

Art.121
(Storage of traffic data for other purposes)

1. Without prejudice to the provisions of Article 112, paragraph 2, telephone traffic data shall be stored by the provider for twenty-four months from the date of communication, for the purposes of detecting and prosecuting crimes, while, for the same purposes, Internet traffic data, excluding the contents of communications, shall be stored by the provider for twelve months from the date of communication.
2. Unanswered call data processed temporarily by providers of publicly available electronic communications services or by a public communication network shall be stored for thirty days.
3. Within the term referred to in paragraph 1, the data shall be acquired from the provider by a reasoned decree of the Judicial Authority also at the request of the defendant's lawyer, the person under investigation, the injured party and other private parties. The defendant's or the person under investigation's lawyer may request, directly to the provider, data relating to his client’s telephone or telematics subscriptions.
4. The Judicial Authority and the Data Protection Authority may order, also in relation to any requests made by foreign investigative authorities, providers and operators of computer or telematics services to store and protect, in the manner indicated and for a period not exceeding ninety days, Internet traffic data, excluding the contents of communications, for the purpose of carrying out preventive investigations, or for purposes of detection and prosecution of specific crimes. The measure, which may be extended, for justified reasons, for a total duration of no more than six months, may provide for special methods of data storage and the possible non-availability of such data from the providers and operators of computer or telematics services or third parties.
5. The provider or operator of computer or telematics services to whom the order referred to in paragraph 4 is addressed shall comply with it without delay and timely inform the requesting authority thereof. The provider or operator of computer or telematics services shall maintain secrecy

with regard to the order received and the activities subsequently carried out for the period indicated by the authority. In case of breach of the obligation of secrecy, the provisions of Article 377 of the Criminal Code shall apply, unless the fact constitutes a more serious crime.

6. The measures adopted pursuant to paragraph 4 shall be communicated in writing, without delay and in any case within forty-eight hours of notification to the recipient, to the Judicial Authority who, if the conditions are met, shall validate them. In the event of non-validation, the measures adopted shall lose their effectiveness.

7. Data processing for the purposes referred to in paragraph 1 shall comply with the measures and safeguards for data subjects prescribed by the Data Protection Authority and designed to ensure that the stored data shall be of the same quality and subject to the same security and protection as those data on the network, as well as to indicate the technical methods for the periodic destruction of data, after the period referred to in paragraph 1.

Art.122

(Procedures established by providers)

1. Providers shall be required to establish internal procedures for responding to requests made in accordance with the provisions which envisage forms of access to users' personal data.

2. Upon request, providers shall transmit the Data Protection Authority, for matters falling within its competence, information about the procedures referred to in paragraph 1, the number of requests received, the legal justification invoked and their response.

Art.123

(Security of processing)

1. In accordance with Article 33, the provisions of this Article shall apply to providers of publicly available electronic communications services.

2. Pursuant to Article 4, paragraph 1), letter f), the provider of a publicly available electronic communications service shall implement technical and organisational measures appropriate to the risk presented, also through other entities entrusted with the provision of the service.

3. Persons operating on electronic communications networks shall ensure that personal data can be accessed only by authorised personnel for legally authorised purposes.

4. The measures referred to in paragraphs 2 and 3 shall ensure the protection of traffic and location data and other personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, as well as the implementation of a security policy.

5. When the security of the service or of personal data also requires the adoption of measures that relate to the network, the provider of the publicly available electronic communications service shall adopt such measures in conjunction with the provider of the public communications network.

Art.124

(Information to subscribers and users)

1. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service shall inform the subscribers and, where possible, the users concerning such risk and any possible remedies, including the costs involved, where the risk is outside the scope of the measures to be adopted by the provider pursuant to Article 123, paragraphs 2, 3 and 5. Similar information shall be provided to the Data Protection Authority.

Art.125

(Amendments to the provisions of this Section)

1. The provisions contained in this Section may be amended by delegated decree.

SECTION V
FINAL PROVISIONS

Art.126
(Data Protection Authority's remuneration and financial coverage)

1. Special chapters shall be established in the State budget for the financial year 2019 to cover the financial costs arising from the implementation of this Law.
2. Remunerations and attendance fees for the members of the Data Protection Authority shall be determined by an *ad-hoc* delegated decree.

Art.127
(Provisions on State and Public Entities' databases)

1. The currently active databases of the State and Public Entities, established and authorised by Decree no. 27 of 13 March 1984, Decree no. 67 of 3 June 1986 and Decree no. 92 of 4 August 2017, shall be hereby confirmed.

Art.128
(Final provisions and repeals)

1. Any provision contrary to this Law shall be repealed, such as:
a) Law no. 70 of 23 May 1995, which remains in force only with regard to the computerised collection of data of legal persons;
b) Article 41 of Law no. 188 of 5 December 2011.
2. Letter d), paragraph 1 of Article 37 of Law no. 188/2011 and subsequent amendments shall be deleted.
3. The reference to the User Data Protection Supervisor referred to in Article 25, paragraph 4, letter b) of Law no. 188/2011 and subsequent amendments shall be understood as referring to the Data Protection Authority mentioned in this Law.
4. In the overall public sector the profiles of controller, processor and data protection officer, referred to in Title IV of this Law, shall be identified by means of a Congress of State decision.

Art.129
(Entry into force)

1. This Law shall enter into force on the fifteenth day following that of its legal publication.

Done at Our Residence, on 21 December 2018/1718 since the Foundation of the Republic

THE CAPTAINS REGENT
Mirco Tomassoni - Luca Santolini

MINISTER OF INTERNAL AFFAIRS
Guerrino Zanotti

The above translation consists of 60 pages.
In witness thereof