3379

GOVERNMENT GAZETTE
OF THE HELLENIC REPUBLIC

29 AUGUST 2019 | SERIES A | ISSUE NO 137

LAW NO. 4624

Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions.

**THE PRESIDENT
OF THE HELLENIC REPUBLIC**

Hereby adopts the following Law which has been passed by the Parliament:

CHAPTER A
GENERAL PROVISIONS

Article 1
Purpose

The purpose of this Law is:

a) to replace the legislative framework governing the establishment and operation of the Data Protection Authority,

b) to adopt measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR),

c) to transpose Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Article 2
Material scope

The provisions of 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 such data, which form part of a filing system or are intended to form part of a filing system carried out by:

(a) public bodies or

(b) private bodies, unless the processing is carried out by a natural person in the course of a purely personal or household activity.

Article 3
Territorial scope

The provisions of this Law shall apply to public bodies. They shall also apply to private bodies, provided that:

(a) the controller or processor processes personal data in the Greek territory,

(b) personal data are processed in the context of the activities of an establishment of the controller or processor within the Greek territory, or if

(c) although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it falls within the scope of the GDPR.

Article 4
Definitions

For the purposes of this Law:

(a) 'public body' means public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first and second-level local government authorities with their legal persons and their legal entities, state-owned or public undertakings and agencies, legal persons governed by private law which are state-owned or regularly receive at least 50% of their annual budget in the form of state subsidies, or their administration is designated by the state,

(b) 'private body' means any natural or legal person or group of persons without legal personality which does not fall within the definition of a 'public body',

(c) 'competent supervisory authority' means the Hellenic Data Protection Authority (hereinafter: the Authority).

Article 5
Legal basis for the processing of personal data by public bodies

Public bodies may process personal data where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority conferred on the controller.

Article 6
Designation of the data protection officer in public bodies

1. Public bodies shall designate a data protection officer (hereinafter: the DPO).
2. A single DPO may be appointed for several public bodies, taking into account their organisational structure and size.
3. The DPO shall be selected 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 8.
4. The DPO may be an employee of the public body in any capacity, or fulfil his or her tasks on the basis of a service contract.
5. The public body shall publish the contact details of the DPO and communicate them to the Authority, unless this is not permitted for reasons of national security or for the purposes of maintaining confidentiality, as provided for by law.

Article 7
Position of the DPO in public bodies

1. The public body shall ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data.
2. The public body shall support the DPO in performing the tasks referred to in Article 8 by providing resources necessary to carry out those tasks, ensuring access to personal data, to processing operations, and to maintain his or her expert knowledge.
3. The public body shall ensure that the DPO does not receive any instructions regarding the exercise of his or her tasks, reports directly to the highest management level of the public body, and is not dismissed or penalised by the controller for performing his or her tasks.
4. Termination of the employment contract of the DPO, or revocation of the duties assigned to him or her, where the DPO is also an employee of the public body, shall only be allowed for good reason. After the expiry of his or her employment contract as a DPO, he or she shall not be dismissed for one (1) year, unless the public body has good reason to terminate his or her contract.
5. The data subjects may consult the DPO on any matter relating to the processing of personal data and the exercise of their rights under the GDPR, this Law and any other legislation on the protection of personal data. The DPO shall be bound by secrecy or confidentiality concerning the identity of data subjects and the circumstances in which conclusions can be drawn as to the data subject, unless the identity of the data subject is disclosed by the subject itself.
6. If the DPO, in performing his or her tasks, becomes aware of personal data for which the head of the public body has the right to refuse to give evidence as a witness for professional reasons, that right shall also apply to the DPO and his or her assistants.

Article 8
Tasks of the DPO in public bodies

1. In addition to his or her tasks under the GDPR, the DPO shall have at least the following tasks:
(a) to inform and advise the public body and the employees, who carry out the processing, of their obligations under the provisions of this Law and any other legislation on the protection of personal data;
(b) to monitor compliance with the provisions of this Law and any other legislation on the protection of personal data, and with the personal data protection policies of the public body, including accountability and the related audits;
(c) to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Article 65;
(d) to cooperate with the Authority;
(e) to act as the contact point with the Authority on issues relating to processing, including the prior consultation referred to in Article 67, and to consult the Authority, where appropriate, with regard to any other matter.
2. The tasks of the DPO, who may be designated by judicial and prosecutorial authorities, shall not concern the processing operations carried out by judicial and prosecutorial authorities acting in their judicial capacity.
3. The DPO may fulfil other tasks and duties. The controller or processor shall ensure that the exercise of any such tasks and duties does not result in a conflict of interests.
4. The DPO shall, in the performance of his or her tasks, have due regard to the risk associated with processing, the nature, scope, context and purposes of processing.

CHAPTER B
SUPERVISORY AUTHORITY

Article 9
Hellenic Data Protection Authority

The Authority, which has been established by Law 2472/1997 (Government Gazette A' 50), shall supervise the application of the provisions of the GDPR, this Law and other regulations relating to the protection of natural persons with regard to the processing of their personal data on the Greek territory. The Authority is an independent public authority under Article 9a of the Constitution and has its seat in Athens.

Article 10
Competence

1. The Authority shall cooperate with the supervisory authorities of Member States of the European Union, and the European Commission.

2. The Authority shall represent Greece in the European Data Protection Board (hereinafter: the EDPB) and other committees or bodies relating to the protection of personal data which involve the participation of a national supervisory authority.

3. The Authority shall cooperate with respective supervisory authorities of third countries and international organisations to meet the objectives specified in Article 50 of the GDPR.

4. In cases where an independent audit or supervision is provided for in international or transnational conventions or in European Law or in national law, the Authority shall exercise its respective competences and powers.

5. The Authority shall not be competent to supervise processing operations of personal data carried out by judicial and prosecutorial authorities acting in their judicial capacity, or processing operations of classified personal data carried out for activities concerning national security.

Article 11
Functional independence

1. The Authority shall be composed of the President and six (6) members, who shall be appointed with their respective alternates. They shall have a six-year non-renewable term of office.

2. Individuals of acknowledged status shall be selected as members and alternates, who are distinguished for their scientific expertise and professional experience in areas related to the mission and competence of the Authority. Greek nationality is a precondition for selection as a member of the Authority.

3. The President, the members of the Authority and their alternates shall be selected and appointed in accordance with Article 101a of the Constitution.

4. The members of the Authority shall be senior state officials, enjoy both personal and functional independence and shall not be subject to any hierarchical or administrative control. They shall exercise their duties and powers free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

5. The President and the Deputy President shall be employed on an exclusive time basis at the Authority. Such status shall entail the suspension of any public function and professional activity.

6. The members of the Authority shall not incur third party civil liability for acts or omissions in the exercise of their powers. They shall be liable to the Greek state for acts or omissions committed intentionally or with gross negligence. The members of the Authority shall not be prosecuted for opinions expressed or for acts or omissions committed in the course of carrying out their duties, unless they acted fraudulently or with gross negligence. The Authority may reimburse the costs of legal defence of its members in the event of an action or criminal proceedings brought against them in respect of acts or omissions resulting solely from the performance of their duties.

Article 12
Impediments — incompatibilities for the members of the Authority

1. A person may not be appointed as a President, Deputy President, or member of the Authority if this person is: (a) a minister, state secretary, general or special secretary of a Ministry or of a separate general or special secretariat and a member of parliament; and (b) a manager or a member of a management body of an undertaking that provides services relating to the processing of personal data or is associated with a project contract of equivalent content.

2. Any kind of professional or other activities relating to the competences of the Authority shall be incompatible with the status of member of the Authority, with the exception of scientific and research activities. The members of the Authority may not appear before the Authority for two (2) years after the expiry of their term of office.

3. The members of the Authority shall be permitted to perform duties of HEI (higher education institutions) teaching staff on a full-time or part-time basis.

4. Any person who, following his or her appointment:

(a) Acquires one of the functions constituting a barrier to appointment referred to paragraph 1.

(b) Engages in actions or undertakes any work or project, or acquires another capacity which, in the Authority's view, is incompatible with his or her duties as a member of the Authority, shall be automatically disqualified as President, Deputy President or member of the Authority.

5. The Authority shall establish the incompatibilities referred to in the previous paragraph, without the participation of the member who may be in one of the situations of incompatibility. The Authority shall reach its decision after hearing the member concerned. The proceedings shall be initiated either by the President of the Authority or by the President of the Parliament.

Article 13
Tasks of the Authority

1. In addition to the Authority's tasks under Article 57 of the GDPR, the Authority shall:

(a) be competent for the monitoring and enforcement of this Law and other regulations relating to the protection of individuals with regard to the processing of personal data,

(b) take appropriate action to promote public awareness and understanding of the risks, safeguards and rights in relation to the processing of personal data,

(c) provide an opinion on any provision to be included in a law or regulatory act relating to the processing of personal data.

The consultation shall take place at the drafting stage of the regulation at a time and in a manner that allows for a timely opinion by the Authority and the relevant consultation on the content of the draft regulation,

(d) issue guidelines and make recommendations on any matter concerning the processing of personal data, without prejudice to the tasks of the EDPB in accordance with

Article 70 of the GDPR,

(e) upon submission of a specific request, inform the data subject of the exercise of his or her rights in accordance with this Law and other regulations for the protection of individuals with regard to the processing of personal data. For that purpose, it shall cooperate with the supervisory authorities of other Member States of the European Union,

(f) issue standard documents and complaint forms,

(g) handle complaints lodged by the data subject, or by a body, organisation or association, and inform the complainant of the progress and the outcome of the investigation or inspection within a reasonable period,

(h) conduct, ex officio or following a complaint, investigations or inspections regarding the application of this Law and other regulations relating to the protection of individuals with regard to the processing of personal data, including on the basis of information received from another public authority,

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular developments in information and communication technologies and commercial practices,

(j) contribute to the activities of the EDPB.

2. In exercising its powers, the Authority shall file without further action any requests, questions or complaints which are manifestly vague, unfounded or understated, or are submitted abusively or anonymously. The Authority shall inform the data subjects and the applicants of its actions. Without prejudice to the time limits set out in the GDPR, the priority for examining requests, questions and complaints shall be assessed by the Authority on the basis of the relevance and general interest of the matter.

Article 14
Activity report

The Authority shall draw up each year a report on the performance of its tasks during the previous calendar year. The report shall be submitted by the President of the Authority to the President of the Parliament and the Prime Minister, and shall be published in the Government Gazette under the responsibility of the Authority, which may give further publicity to the report.

Article 15
Investigative and corrective powers

1. In addition to the powers laid down in Article 58 of the GDPR, the Authority shall conduct, ex officio or following a complaint, investigations and audits relating to the compliance with this Law during which the technological infrastructure and other automated or non-automated means supporting the processing of personal data are subject to controls. In carrying out such investigations and inspections, the Authority shall have the power to obtain, from the controller and the processor, access to all personal data processed and to all information necessary for the purposes of such audits and the performance of its tasks, and no type of confidentiality may be relied upon against it. The Authority shall, by way of exception, not have access to data identifying associates or staff employed in entities contained in records held for national security purposes or for the purpose of investigating particularly serious crimes.

2. The audits shall be carried out by a member or members of the Authority, or employees of the Secretariat's department of scientific staff who are specially authorised to that effect by the President of the Authority. The President and the members of the Authority, as well as the Secretariat's specially mandated officials shall be deemed as special investigating officers having all the rights provided for in the Code of Criminal Procedure. They shall be entitled to carry out a preliminary investigation, even without an order by the Public Prosecutor, in case of an act caught in flagrante delicto, or a misdemeanor, or if there is a risk as a result of any delay. The public authorities shall assist the Authority in carrying out the audit.

3. The President of the Authority may grant the power to carry out audits to members and staff of a supervisory authority of another Member State of the European Union ('seconding supervisory authority') in the framework of joint operations carried out under Article 62 of the GDPR and Article 79 of this Law.

4. The Authority shall, for the purposes of this Law:

(a) issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Law;

(b) order the controller or processor to comply with the provisions of this Law in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data;

(c) order and impose a temporary or definitive limitation, or even a ban on the processing of personal data;

(d) order and impose that documents, filing systems, equipment or means for processing personal data be delivered to it, as well as their content in the case provided for in subparagraph (c) of this paragraph;

(e) seize documents, information, filing systems for each piece of equipment and means of personal data breach, and their content which becomes known to the Authority in the exercise of its supervisory powers. The Authority shall be the sequestrator of the above material until a decision has been reached by the competent judicial and prosecutorial authorities.

5. In addition to the corrective powers provided for in Article 58(2) of the GDPR, the Authority shall order the controller or processor, or a recipient, or a third party, to discontinue the processing of personal data or to return or lock (block) the relevant data or to destroy the filing system or the relevant data.

6. The Authority shall impose the administrative penalties provided for in Article 83 of the GDPR and Article 39 hereof.

7. The Authority shall impose the administrative penalties provided for in Article 82.

8. Where the protection of the individual against the processing of personal data concerning him or her requires immediate decision-making, the President may, at the request of the person concerned or ex officio, issue a temporary order for immediate temporary limitation, in whole or in part, of the processing or the operation of the file. The order shall apply until the Authority reaches its final decision.

9. In order to ensure compliance with the provisions of

the GDPR, this Law and other regulations relating to the protection of the data subject with regard to the processing of personal data, the Authority, without prejudice to Chapter VII of the GDPR, shall adopt administrative regulatory acts to regulate specific, technical and detailed matters referred to in those acts.

10. The regulatory acts of the Authority, which shall not be published in the Government Gazette, shall be published on the Authority's website.

Article 16
Rights and obligations of the members of the Authority

1. In performing their tasks, the President and the members of the Authority shall be subject to their conscience and the law, and have a duty of confidentiality. As witnesses or expert witnesses they may testify only on facts exclusively and solely pertaining to the compliance with the provisions of the GDPR and this Law. The duty of confidentiality shall be upheld even after the President and the members of the Authority have in any way retired.

2. For a period of two (2) years after the expiry of their term of office, the President and the members of the Authority shall not be partners, shareholders, board members, technical or other consultants, or be employed with or without remuneration on a salaried assignment basis or in any legal relationship, in a company or an undertaking whose activities have been subject, directly or indirectly, to the control of the Authority during their term of office, provided that they have been in any way involved in such control. The same prohibition applies in the case of complaints submitted to the Authority.

3. Article 18(3) of Law 2472/1997 shall apply to the disciplinary liability of the President and the members of the Authority.

4. The President or a member of the Authority who, in breach of this Law, discloses, in any way whatsoever, personal data accessible to him or her in the course of his or her duties, or allows such data to become known to a third party, shall be punished by imprisonment for a period of up to two (2) years, and a fine. If, however, he or she has committed the act with the purpose of gaining unlawful benefit on his or her behalf, or on behalf of another person, or for the purpose of causing harm to another person, then he or she shall be punished by imprisonment for a period of at least two (2) years, and a fine.

Article 17
Operation of the Authority

1. The Authority may also act as a single-member body (President) or sit in chambers composed of at least three (3) members or alternates, and chaired by the President of the Authority or his/her alternate. Employees of the Auditors Department shall be allowed to attend sessions and meetings of the plenary and the chambers for cases to which they have been appointed assistant rapporteurs.

2. The Authority shall adopt its rules of procedure laying down, in particular, the terms of operation in plenary and chambers, the allocation of duties between the plenary and the chambers, the responsibilities of the single-member body, and the assignment of such responsibilities by the President to the Deputy Chair and to members, both full and alternate, the procedure for convening and conducting a meeting and a decision-making process, the prior hearing of the persons concerned, the procedure for processing and handling cases, the methods in place to carry out audits, and matters relating to the disciplinary procedure. The rules of procedure shall be published in the Government Gazette. The current rules of procedure (Decision 209/6.3.2000 (Government Gazette B' 336) of the President of the Authority, as amended and in force) shall apply until the Authority adopts new rules of procedure.

3. A code of conduct for the members and staff of the Authority shall be adopted by a decision of the Plenary.

4. The Authority may conclude memoranda of understanding with higher education institutions, other public bodies and local authorities with the purpose of ensuring a mutual exchange of information and mutual assistance on matters within its competence. Mutual assistance shall include, in particular, the provision of information and the conduct of investigations and studies, assistance in investigations and audits, and the conduct of inspections on the basis of questions compiled by the Authority.

5. The Authority may offer paid traineeships to students and graduates of higher education institutions whose field of study is relevant to the Authority's duties. The terms and conditions for the selection of trainees, the performance of traineeships, as well as the conditions and the amount of the grant awarded, which is covered by the Authority's budget, shall be set out by a decision of the Authority.

Article 18
Secretariat of the Authority

1. The staff of the Authority shall be appointed under a public or private law employment relationship of unlimited duration to positions set out in the Organisational Chart of the Authority and selected in accordance with Article 4(1) of Law 3051/2002 (Government Gazette A' 220).

2. Staff members of the Auditors Department may not appear before the Authority for two (2) years after the expiry of their employment relationship with the Authority.

3. The Organisational Chart of the Authority setting out the level of operation of the Secretariat, the structure of the organisational units in directorates, departments and offices, the qualifications of the staff, the number of positions, the allocation of such positions in branches and specialties, the setting up of new positions and any other relevant matter shall be stipulated by a presidential decree issued following a proposal of the Minister of Justice and the Minister for Internal Affairs, following an opinion of the Authority. The Organisational Chart also provides for the requirements, the bodies and the procedure for selecting the head of the Secretariat, as well as the heads of the Authority's organisational units. The Organisational Chart also provides for derogations from the applicable provisions in order for the relevant arrangements to comply with the GDPR. Any amendment to the above presidential decree shall require the prior opinion of the Authority. Until the

presidential decree referred to in the previous subparagraph is issued, presidential decree 207/1998 on the organisation of the Secretariat of the Data Protection Authority and the establishment of permanent posts (Government Gazette A' 164) shall apply.

4. Without prejudice to the specific regulations of this Law, the Organisational Chart of the Authority and its Rules of Procedure, the Staff Regulations of the Authority shall be governed by the provisions of Article 4(2) to (7) of Law 3051/2002, as applicable, irrespective of their category, branch and formal qualifications.

5. Article 11(6) shall apply accordingly to the staff of the Authority.

6. In order to meet urgent needs of the Authority's Secretariat, permanent staff or staff employed on private law employment contracts of indefinite duration may be seconded from Central Administration bodies, as defined in indent (f) of Article 14(1) of Law 4270/2014 (Government Gazette A' 143), by derogation from the applicable provisions. The duration of secondments shall be one (1) year renewable once. The secondment shall be carried out following a joint decision of the competent Minister and the President of the Authority without the opinion of the respective Boards of Employees. Prior agreement of the competent appointing bodies shall be specifically sought for the secondment of first and second-level local government authority staff.

7. Secretariat staff may be seconded to supervisory authorities of the Member States, or to the Greek Permanent Representation, or to authorities of third countries or international organisations for a period of up to six (6) months following a decision of the Authority applying the provisions applicable to staff seconded to EU institutions. In addition, staff from the Authority's counterparts may also be seconded to the Authority for a period of up to six (6) months.

8. The university graduate Communications Department positions at the Data Protection Authority shall be converted into equivalent scientific staff positions recruited under a private law employment contract of indefinite duration. Already serving staff who holds the qualifications required under Presidential Decree No 50/2001 (Government Gazette A' 39) "Determining the qualifications for appointment in public service positions" and the legislation in force for the position of scientific staff under a private law employment contract, shall state whether they agree to be assigned to that position or not within one month of the entry into force of this Law. Staff willing to serve under a private law contract, who occupy one of the positions converted, shall maintain their insurance status and count the duration of previous relevant employment towards their grading and salary classification in accordance with the provisions of Article 11(4) of Law 4354/2015 (Government Gazette A' 176). In case of refusal or failure to submit a statement, the members of staff shall continue to serve as permanent university graduate Communications Officers in personal non-transferable positions. In the period during which the members of staff serve in personal non-transferable positions pursuant to the previous subparagraph, no equivalent positions of scientific staff shall be filled under a private law employment contract of indefinite duration.

Article19
Budget and Financial management

1. The Authority shall establish its own budget under the responsibility of its President and shall enjoy full independence in implementing it. The involvement of another body shall not be required in this regard. The President of the Authority shall be the authorising officer.

2. The budget shall be established annually and submitted directly to the State General Accounting Office in accordance with the procedure set out in the Public Accounting.

3. The Authority, in enjoying full independence, shall be solely responsible for implementing its budget. The transfer of appropriations from one account to another and between different major budget categories shall be allowed, depending on the needs of the Authority, by a decision of the Minister of Finance, provided that the total amount of the budget initially approved by the Parliament is not modified. Expenditure incurred by the Authority shall be carried out by the authorising officers and the public accounting in accordance with the relevant applicable provisions of the commitment. The transfer of appropriations shall be carried out following a decision of the Authority and shall be notified to the State General Accounting Office.

4. The budget of the Authority may be amended following a decision of the Minister for Finance, upon recommendation of the Authority, which is submitted to the State General Accounting Office.

5. The Authority may participate in national, European or co-financed research or other programmes. To this end, the Authority may, following a decision of its President, open a regular bank account under the Group of Accounts 260 — Cash Management with the Bank of Greece, to which appropriations will be transferred from those programmes, as well as from other resources related to the exercise of its powers provided for under the GDPR or the law. The management and control of the above special account shall be regulated by the special provision of Article 2(3) of Law 3051/2002. The Authority shall enjoy full independence in the management of this account. The revenue of the Authority shall constitute state budget revenue.

6. Where members and staff of the Authority participate in collective bodies established in the context of projects financed by the European Structural and Investment Funds or the Public Investment Programme, the provisions of Article 21(2), (3) and (5) of Law 4354/2015 (Government Gazette A' 176) shall apply accordingly, provided that the relevant expenditure is borne by these sources of funding and does not place a burden on the state budget.

7. The financial audit of the Authority shall be conducted in a way that does not interfere with its operation nor does it affect its independence.

Article 20
Legal protection against the Authority

1. Regulatory decisions and individual administrative acts issued by the Authority, including decisions imposing penalties, shall be challenged by way of action for annulment before the Council of State.

2. The period of time for lodging an action for annulment shall not have suspensive effect on the contested act. The court may, at the request of the applicant, suspend the execution of the act in whole or in part, in accordance with the provisions in force.

3. An action for annulment against the decisions and acts of the Authority may also be brought by the competent Minister.

4. The Authority shall be represented in and out of court by its President. The Authority shall be an autonomous party to any kind of court proceedings with the participation of its members in their capacity as lawyers or its legal service, provided the legal service is set up. The Authority's legal service shall be staffed by lawyers with a salaried mandate recruited in accordance with the provisions of the Code of Lawyers. The Authority may also be represented on a case-by-case basis by lawyers specialised in their subject matter by means of a reasoned decision providing the relevant power of attorney.

CHAPTER C
SUPPLEMENTARY MEASURES FOR THE IMPLEMENTATION OF THE GDPR REGARDING THE PROCESSING OF PERSONAL DATA

Article 21
Consent of minors

1. Where point (a) of Article 6(1) applies, in relation to the offering of information society services directly to a minor, the processing of the personal data of a minor shall be lawful where the minor is at least 15 years old and gives his or her consent.

2. Where the minor is below the age of 15 years, the processing referred to in paragraph 1 shall be lawful only if consent is given by the legal representative of the minor.

Article 22
Processing of special categories of personal data

1. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR by public and private bodies shall be allowed, if necessary:

(a) for the purpose of exercising the rights arising from the right to social security and social protection, and for fulfilling the obligations arising therefrom;

(b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems or pursuant to a contract with a health professional or other person who is subject to a duty of professional secrecy or supervised by him/her; or

(c) 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, in addition to the measures referred to in the second subparagraph of paragraph 3, the provisions ensuring professional secrecy provided for in a law or code of conduct must in particular be complied with.

2. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data by public bodies within the meaning of Article 9(1) of the GDPR shall be allowed, where it is:

(a) strictly necessary for reasons of essential public interest;

(b) necessary for the prevention of major threats to national or public security; or

(c) necessary for taking humanitarian action, in which case the interests in the processing override the interests of the data subject.

3. In the cases referred to in the previous paragraphs, all appropriate and specific measures shall be taken to safeguard the interests of the data subject. 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 severity for rights and freedoms of natural persons posed by the processing, such measures may include in particular:

(a) technical and organisational measures to ensure that the processing complies with the GDPR;

(b) measures to ensure that ex post verification and determination of whether and by whom personal data have been entered, amended or removed is possible;

(c) measures to raise awareness among staff involved in the processing;

(d) access rights restrictions to controllers and processors;

(e) pseudonymisation of personal data;

(f) encryption of personal data;

(g) measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services relating to the processing of personal data, including the ability to rapidly restore the availability and access in the event of a physical or technical incident;

(h) procedures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

(i) specific rules to ensure compliance with this Law and the GDPR in case of transfer or processing for other purposes;

(j) designation of a DPO.

Article 23
Processing of genetic data

The processing of genetic data for health and life insurance purposes shall be prohibited under Article 9(4) of the GDPR.

Article 24
Processing of personal data for other purposes by public bodies

1. The processing of personal data by public bodies for a purpose other than that for which they were collected shall be permitted where such processing is necessary for the performance of the tasks assigned to them and provided that it is necessary:

(a) for the verification of the information provided by the data subject because there are reasonable grounds for

believing that such information is incorrect;

(b) for the prevention of risks to national security, defence or public security, or for securing tax and customs revenue;

(c) for the prosecution of criminal offences;

(d) for the prevention of serious harm to the rights of another person;

(e) for the production of official statistics.

2. The processing of special categories of personal data, as referred to in Article 9(1) of the GDPR, for a purpose other than that for which they have been collected, shall be permitted provided that the conditions set out in the previous paragraph are fulfilled and one of the exemptions provided for in Article 9(2) of the GDPR or Article 22 of this Law applies.

Article 25
Processing of personal data for other purposes by private bodies

1. The processing of personal data by private bodies for a purpose other than that for which they have been collected shall be permitted, where necessary:

(a) for the prevention of threats to national or public security at the request of a public body; or

(b) for the prosecution of criminal offences; or

(c) for the establishment, exercise or defence of legal claims, unless the interests of the data subject override the grounds for the processing of those data.

2. The processing of special categories of personal data, as referred to in Article 9(1) of the GDPR, for a purpose other than that for which they have been collected, shall be permitted, provided that the conditions set out in the previous paragraph are fulfilled and one of the exemptions provided for in Article 9(2) of the GDPR or Article 22 of this Law applies.

Article 26
Transfer of personal data by public bodies

1. The transfer of personal data by a public body to another public body shall be permitted, where necessary for the performance of the tasks of the transmitting body or the third party to whom the data were transferred, provided that the conditions enabling the processing under Article 24 are met. The third party to whom the data have been transferred shall process them only for the purpose for which they were transferred. Processing for other purposes shall be permitted only if the conditions laid down in Article 24 are met.

2. Public bodies shall be permitted to transfer personal data to private bodies, provided that:

(a) the transfer is necessary for the performance of the tasks of the body transferring the data, and the conditions set out in Article 24 are met;

(b) the third party to whom the data have been transferred has a legitimate interest in being aware of the transfer, and the data subject does not have a legitimate interest in not transferring the data relating to him or her; or

(c) the processing is necessary for the establishment, exercise or defence of legal claims and the third party has pledged to the public body which has transferred the data that he or she will process the data only for the purpose for which they were transmitted. Processing for other purposes shall be permitted if the transfer is authorised in accordance with paragraph 1 and the transmitting body has consented to the transfer.

3. The transfer of special categories of personal data within the meaning of Article 9(1) of the GDPR shall be permitted provided that the conditions set out in paragraph 1 or paragraph 2 are met and one of the exemptions in Article 9(2) of the GDPR or in accordance with Article 22 hereof applies.

Article 27
Processing of personal data in the context of employment

1. Employees' personal data may be processed for the purposes of the contract of employment where the processing is strictly necessary for deciding whether to enter into a contract of employment, or for the performance of a contract of employment once it has been concluded.

2. Where an employee's consent is, by way of exception, used as the legal basis for the processing of the employee's personal data, the following should be taken into account in deciding whether consent was freely given, and in particular:

(a) the employee's dependence, as set out in the contract of employment and

(b) the circumstances under which consent was given. Consent can be given either in writing or in electronic form and must be clearly distinguishable from the contract of employment. The employer must inform the employee, either in writing or in electronic form, about the purpose of the processing of the employee's personal data and his or her right to withdraw consent under Article 7(3) of the GDPR.

3. By way of derogation from Article 9(1) of the GDPR, processing of special categories of personal data within the meaning of Article 9(1) of the GDPR for the purposes of the contract of employment shall be permitted if it is necessary for the exercise of their rights or for compliance with legal obligations arising from employment, social security and social protection law, and there is no reason to believe that the data subject's legitimate interests in relation to processing take precedence. Paragraph 2 shall also apply to consent given for the processing of special categories of personal data. Consent should explicitly refer to such data. Article 22(3)(b) shall apply accordingly.

4. The processing of personal data, including special categories of the employees' personal data, shall be permitted for the purposes of the contract of employment on the basis of collective labour agreements. The negotiating parties shall comply with Article 88(2) of the GDPR.

5. The controller shall take appropriate measures to ensure that, in particular, the principles for the processing of personal data laid down in Article 5 of the GDPR are complied with.

6. Paragraphs 1 to 5 shall also apply where personal data, including special categories of employees' personal data, are subject to processing, without being stored or intended to be stored in a filing system.

7. Processing of personal data through closed circuit television systems in the workplace, whether publicly accessible or not, shall only be permitted if it is necessary for the protection of persons and goods. Data collected through a closed circuit television system cannot be used as a criterion for assessing the performance of employees. The employees shall be informed in writing or electronically of the installation and operation of a closed circuit television system in the workplace.

8. For the purposes of this Law, employees mean workers recruited under any type of employment relationship, or a work contract, or a service contract in the public and private sector, regardless of the validity of the contract, as well as job applicants and former workers.

Article 28
Processing and freedom of expression and information

1. To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the processing of personal data is allowed where:

(a) the data subject has given his or her explicit consent, (b) it relates to personal data which are manifestly made public by the data subject, (c) the right to freedom of expression and the right to information override the right to the protection of the data subject's personal data, in particular on matters of general interest or where it relates to personal data of public figures, and (d) where it is limited to what is necessary to ensure freedom of expression and the right to information, in particular with regard to special categories of personal data, criminal proceedings, convictions and related security measures, taking into account the right of the data subject to his or her private and family life.

2. To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the following shall not apply: (a) Chapter II of the GDPR (principles), except for Article 5, (b) Chapter III of the GDPR (rights of the data subject), c) Chapter IV of the GDPR (controller and processor), except for Articles 28, 29 and 32, (d) Chapter V of the GDPR (transfer of personal data to third countries or international organisations), (e) Chapter VII of the GDPR (cooperation and consistency) and f) Chapter IX of the GDPR (specific data processing situations)".

Article 29
Processing of personal data for archiving purposes in the public interest

1. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR shall be allowed where it is necessary for archiving purposes in the public interest. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests. Such measures may include, as far as possible, in particular:

(a) access rights restrictions to controllers and processors;

(b) pseudonymisation of personal data;

(c) encryption of personal data;

(d) designation of a DPO.

2. By way of derogation from Article 15 of the GDPR, the data subject's right of access to data relating to him or her may be restricted where the exercise of that right is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1, and the exercise of the right would entail a disproportionate effort.

3. By way of derogation from Article 16 of the GDPR, the data subject shall not have the right to have the personal data relating to him or her rectified where the exercise of that right is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 or the exercise of the rights of others.

4. By way of derogation from subparagraphs (a), (b) and (d) of Article 18(1), and from Articles 20 and 21 of the GDPR, the rights of the data subject shall be restricted where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for the achievement of such objectives.

Article 30
Processing of personal data for scientific or historical research purposes or for the collection and maintenance of statistical information

1. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data, within the meaning of Article 9(1) of the GDPR, shall be allowed without the consent of the data subject where the processing is necessary for scientific or historical research purposes, or for the collection and maintenance of statistical information, and the interest of the controller is overriding the interest of the data subject in not having his or her personal data processed. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests. Such measures may include, in particular:

(a) access rights restrictions to controllers and processors;

(b) pseudonymisation of personal data;

(c) encryption of personal data;

(d) designation of a DPO.

2. By way of derogation form the provisions of Articles 15, 16, 18 and 21 of the GDPR, the rights of the data subject shall be limited where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for their achievement. For the same reason, the data subject's right of access provided for in Article 15 of the GDPR shall not apply where personal data are necessary for scientific purposes and the provision of information would entail a disproportionate effort.

3. In addition to what is referred to in paragraph 1, special categories of personal data, where processed for the purposes of paragraph 1 shall, unless it is contrary to the legitimate interest of the data subject, be anonymised as soon as the scientific or statistical purposes allow. Until then, the characteristics that can be used to match individual details associated with personal or real situations of an identified or identifiable person must be stored separately. These characteristics can only be combined with individual details if required for research or statistical purposes.

4. The controller may publish personal data processed in the context of research, if the data subjects have given their consent in writing or the publication is necessary for the presentation of the results of the research. In the latter case, the results shall undergo pseudonymisation before being published.

Article 31
Information to be provided where personal data are collected from the data subject

1. The obligation to inform the data subject pursuant to Article 13(3) of the GDPR shall not apply, with the exception of the exemption referred to in Article 13(4) of the GDPR where the information to be provided on further processing:

(a) concerns further processing of data stored in a written form in which the controller directly addresses the data subject, the purpose is compatible with the original purpose of collection in accordance with the GDPR, communication with the data subject is not in digital form and the interest of the data subject in being informed according to the circumstances of the case, in particular as regards the context in which the data have been collected, is not deemed to be high;

(b) in the case of a public body, would compromise the proper performance of the controller's tasks within the meaning of points (a) to (e) of Article 23(1) of the GDPR, and the interest of the controller in not providing information overrides the data subject's interest;

(c) would compromise national or public security, and the interest of the controller in not providing information overrides the data subject's interest;

(d) would prevent the establishment, exercise or defence of legal claims, and the interest of the controller in not providing information overrides the interest of the data subject;

(e) would compromise the confidentiality of the data transfer to public bodies.

2. Where no information is given to the data subject in accordance with paragraph 1, the controller shall take appropriate measures to protect the data subject's legitimate interests, including the provision to the public of the information referred to in Article 13(1) and (2) of the GDPR in an accurate, transparent, intelligible and easily accessible form, in clear and plain language. The controller shall state in writing the reasons for forgoing the provision of information. The above subparagraphs shall not apply to indents (d) and (e) of the previous paragraph.

3. Where no notification is given in the cases referred to in paragraph 1 due to a temporary obstacle, the controller, taking into account the specific conditions of the processing, should comply with the obligation to provide information within a reasonable period of time after the obstacle has been removed, but not later than a period of two (2) weeks.

4. If, at the start of a mandate or in the course of a mandate, the customer disclosed data of third parties to an entity bound by an obligation of professional secrecy, the transmitting entity shall not be required to provide information to the data subject in accordance with Article 13(3) of the GDPR, unless the interest of the data subject in obtaining the information is overriding.

Article 32
Information to be provided where the personal data have not been obtained from the data subject

1. The obligation to inform the data subject in accordance with Article 14(1), (2) and (4) of the GDPR shall not apply where the provision of information:

(a) in the case of public bodies:

(aa) would compromise the proper performance of the controller's tasks within the meaning of points (a) to (e) of Article 23(1) of the GDPR, or

(bb) would compromise national or public security;

and, therefore, the data subject's interest in obtaining the information recedes,

(b) in the case of private bodies:

(aa) would prejudice the establishment, exercise or defence of legal claims, or the processing includes personal data resulting from contracts established under private law and is aimed at preventing damages caused by criminal offences, unless the data subject has an overriding legitimate interest in obtaining the information; or

(bb) the competent public authority has specified to the controller that the publication of the data would compromise national defence, national security and public security, while in the case of data processing for law enforcement purposes, specification pursuant to the first subparagraph is not required.

2. Where no information is provided to the data subject in accordance with paragraph 1, the controller shall take appropriate measures to protect the data subject's legitimate interests, including the provision to the public of the information referred to in Article 14(1) and (2) of the GDPR in an accurate, transparent, intelligible and easily accessible form, in clear and plain language. The controller shall state in writing the reasons for which he or she has refrained from providing information.

3. The obligation to provide information to the data subject in accordance with Article 14(1) to (4) of the GDPR, with the exception of exemptions referred to in Article 14(5) of the GDPR, shall not apply insofar as, by fulfilling this obligation, information would be disclosed which by its nature, in particular due to overriding legitimate interests of third parties, should remain confidential.

Article 33
Right of access by the data subject/Communication of a personal data breach to the data subject

1. In addition to the exemptions laid down in Article 29(2) and Article 30(2), the right of access by the data subject

in accordance with Article 15 of the GDPR shall not apply, where:

(a) the data subject is not informed in accordance with point (bb) of indents (a) and (b) of paragraph 1 of the previous Article; or

(b) the data

(aa) were recorded only because they cannot be erased due to retention requirements provided for in legal or regulatory provisions, or

(bb) only serve purposes of protection or control of data,

and the provision of information would require a disproportionate effort, and the necessary technical and organisational measures render impossible their processing for other purposes.

2. The grounds for refusing to provide information to the data subject should be documented. Refusal to provide information should be justified to the data subject unless the disclosure of the factual or legal reasons on which the refusal is based would compromise the purpose pursued by the refusal to provide information. Data stored for the purpose of providing information to the data subject and for the preparation of such provision may be processed solely for that purpose and for purposes of data protection; the processing for other purposes shall be limited in accordance with Article 18 of the GDPR.

3. The right of access by the data subject to personal data that are neither subject to automated nor to non-automated processing by a public authority, and stored in a filing system, shall only apply if the data subject provides information allowing the retrieval of data and the effort required to provide the information is not disproportionate to the interest of the data subject in being informed.

4. The data subject's right to be informed under Article 15 of the GDPR shall not apply to the extent that the provision of information would entail the disclosure of information which, according to the law or by reason of its nature, in particular due to overriding legitimate interests of third parties, should remain confidential.

5. The obligation to notify under Article 34 of the GDPR, with the exception of the exemption referred to in Article 34(3) of the GDPR, shall not apply to the extent that the obligation to notify would entail the disclosure of information which, according to the law or by reason of its nature, in particular due to overriding legitimate interests of third parties, should remain confidential. By way of derogation from the previous subparagraph, the data subject must be informed, in accordance with Article 34 of the GDPR, where his or her interests, in particular taking into account imminent damage, override the interest relating to maintaining confidentiality.

Article 34
Right to erasure

1. If, in the case of non-automated processing, erasure is not possible due to the particular nature of storage or is only possible with disproportionate effort, and the interest of the data subject in erasure is not considered significant, the data subject's right and the controller's obligation to erase personal data in accordance with Article 17(1) of the GDPR, shall not apply, with the exception of the exemptions referred to in Article 17(3) of the GDPR. In this case, erasure shall be replaced by restriction of processing in accordance with Article 18 of the GDPR. The above subparagraphs shall not apply if the personal data have been unlawfully processed.

2. In addition to points (b) and (c) of Article 18(1) of the GDPR, the first and second subparagraphs of the previous paragraph shall apply accordingly in the case of points (a) and (d) of Article 17(1) of the GDPR, to the extent that the controller has reason to believe that the erasure would be prejudicial to the legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing where such information is not impossible or does not involve a disproportionate effort.

3. In addition to point (b) of Article 17(3) of the GDPR, paragraph 1 shall apply accordingly in the case of point (a) of Article 17(1) of the GDPR, if erasure would be in conflict with statutory or contractual retention periods.

Article 35
Right to object

The right to object under Article 21(1) of the GDPR shall not be applicable where a public body is concerned, if there is a compelling public interest in the processing which overrides the interests of the data subject or if processing is mandatory by law.

Article 36
Ensuring the processing of personal data for national security purposes

The processing of personal data of the National Intelligence Service (NIS) staff conducted by public and private bodies in the context of their tasks or responsibilities shall be performed by specifically authorised officers, whose names shall be communicated to the NIS.

Any further transmission of the above personal data shall only be conducted upon approval of the NIS.

Article 37
Accreditation of certification bodies and certification

1. The accreditation of bodies which issue certifications under Article 42 of the GDPR shall be carried out by the National Accreditation System (ESYD) in accordance with EN-ISO/IEC17065:2012 and additional requirements established by the Authority.

2. The ESYD shall revoke an accreditation if notified by the Authority that the requirements for accreditation are no longer met or the certification body infringes the GDPR and the provisions hereof.

Article 38
Criminal penalties

1. Anyone who, without legal grounds: (a) interferes in any way with a data filing system and in so doing is made aware of such data; (b) copies, removes, alters, harms, collects, registers, organises, structures, stores,

adapts, modifies, recovers, seeks information, correlates, combines, restricts, erases, destroys, shall be punished with imprisonment of up to one (1) year, unless the act is punishable with a more severe penalty under another provision.

2. Anyone who uses, transmits, disseminates, discloses by transmission, makes available, announces or makes accessible to unauthorised persons personal data acquired pursuant to indent (a) of paragraph 1, or allows unauthorised persons to become aware of such data, shall be punished with imprisonment, unless the act is punishable with a more severe penalty under another provision.

3. If the act referred to in paragraph 2 relates to special categories of personal data referred to in Article 9(1) of the GDPR or data relating to criminal convictions and offences or relevant security measures referred to in Article 10 of the GDPR, the offender shall be punished with imprisonment of at least one (1) year and a fine of up to one hundred thousand euros (EUR 100,000), unless the act is punishable with a more severe penalty under another provision.

4. The person who has committed the acts referred to in the previous paragraphs shall be punished with incarceration of up to ten (10) years, if he or she intended to secure for himself or herself or others an unjust profit, or cause financial loss to another person, or cause damage to another person, and the total profit or total loss exceeds the amount of one hundred and twenty thousand euros (EUR 120,000).

5. If the acts referred to in paragraphs 1 to 3 have resulted in a risk to the free functioning of democracy or national security, they shall be punishable with imprisonment and a fine of up to three hundred thousand euros (EUR 300,000).

6. The felonies provided for in this Article shall fall within the jurisdiction of the three-member court of appeal for felonies.

Article 39
Administrative sanctions

1. Without prejudice to the Authority's corrective powers in accordance with Article 58(2) of the GDPR, the Authority may, in a specific reasoned decision and following a previous notice summoning the interested parties to provide explanations, impose to bodies of the public sector, as this is defined in indent (a) of Article 14(1) of Law 4270/2014 (Government Gazette A' 143), with the exception of public undertakings and bodies referred to in Chapter A of Law 3429/2005 (Government Gazette A' 314), in their capacity as data controllers, for infringements relating to:

(a) indent (a) of Article 83(4) of the GDPR, with the exception of Articles 8, 27, 29, 42, 43 of the GDPR, (b) Article 83(5) and (6) of the GDPR, with the exception of Articles 17, 20, 47, 90 and 91 of the GDPR, (c) Articles 5, 6, 7, 22, 24, 26, 27 (with the exception of paragraph 7 thereof), Articles 28 to 31, and indent (a) of Article 32(1), Articles 33 to 35 of this Law, an administrative fine of up to ten million euros (EUR 10,000,000).

2. When deciding whether to impose an administrative fine and determining its amount, 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 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) any action taken by the body of the public sector to mitigate the damage suffered by data subjects,

(c) any relevant previous infringements by the body of the public sector,

(d) the categories of personal data affected by the infringement,

(e) the manner in which the infringement became known to the Authority, in particular whether, and if so to what extent, the body of the public sector notified the infringement and

(f) where measures referred to in Article 58(2) of the GDPR have previously been ordered against the body of the public sector, with regard to the same infringement, the degree of compliance with those measures.

3. If a body of the public sector, for the same or linked processing operations, infringes several provisions of the GDPR or of this Law, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

Article 40
Judicial remedy against a controller or processor

1. Actions brought by a data subject against a controller or processor for breach of data protection provisions within the scope of the GDPR or the rights of the data subject referred to therein shall be brought before the civil courts in whose district the controller or processor has his or her establishment. The actions referred to in the previous subparagraph may also be brought before the civil courts in whose district the data subject has his or her habitual residence.

2. The previous paragraph shall not apply to actions brought against public authorities, where such authorities exercise sovereign power conferred on them.

3. Where the controller or processor has designated a representative in accordance with Article 27(1) of the GDPR, the representative in question shall be considered to be a procedural representative for the serving of all documents carried out in the framework of civil proceedings pursuant to paragraph 1.

Article 41
Representation of a data subject

1. Where the data subject considers that the processing of personal data relating to him or her infringes the provisions of the GDPR or Chapter III of this Law, he or she shall have the right to mandate a not-for-profit body, organisation, association or a not-for-profit group of persons without legal personality which has been properly constituted and is legally established in the Greek territory, has statutory objectives which are in the public interest and is active in the area of protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge a complaint on his or her behalf with the Authority in accordance with Article 77 of the GDPR, and to exercise on his or her behalf the rights referred to in Article

78 of the GDPR and Article 20 of this Law.

2. The representation mandate referred to in paragraph 1 shall be made by means of a specific written authorisation validated for the signature authenticity of the contracting party in accordance with Article 11(1)(a) of the Code of Administrative Procedure (Law 2690/1999, Government Gazette A' 45). The mandate may be revoked at any time, in whole or in part.

Article 42
Public access to documents

1. The application of the provisions of Article 5 of the Code of Administrative Procedure relating to the provision of documents by bodies of the public sector falling within the scope of Article 1 of the above Code and of other provisions relating to the issuing of documents by the body or authority or agency concerned shall remain unaffected, where those documents are personal data.

2. The application of the provisions of Article 22 of the Code of court organisation and status of judicial officials (Law 1756/1988, Government Gazette A' 35) shall remain unaffected.

CHAPTER D
TRANSPOSITION OF DIRECTIVE (2016/680)

SECTION I
SCOPE — GENERAL PRINCIPLES

Article 43
Scope
(Articles 1 and 2 of the Directive)

The provisions of this Chapter shall apply to the processing of personal data by public authorities which are competent for 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. In the above cases, the public authorities are always considered as controllers. Where, in this Chapter, provisions for processors are included, its provisions shall also apply to them.

Article 44
Definitions
(Article 3 of the Directive)

1. For the purposes of this Chapter:

(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 in 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 public authority which, alone or jointly with others, determines the purposes and means of the processing of personal data;

(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. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union law or any other law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(j) '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 processed;

(k) '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;

(l) '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;

(m) '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;

(n) 'special categories of personal data' means 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;

(o) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;

(p) '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 countries;

(q) 'consent' means any freely given, specific for the purposes of the case, unambiguous and informed 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.

Article 45
General Principles
(Article 4 of the Directive)

1. Personal data must be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step provided for by provisions in force 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 they are processed;

(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 must be able to demonstrate compliance with his or her obligations pursuant to the previous paragraph.

SECTION II
LEGAL BASES FOR PROCESSING

Article 46
Processing of special categories of personal data
(Article 10 of the Directive)

1. Processing of special categories of personal data shall only be allowed where strictly necessary for the performance of the tasks of the controller.

2. Where special categories of personal data are processed, appropriate safeguards for the data subject's protected legitimate interests shall apply. Appropriate safeguards may include in particular:

(a) specific requirements for data security or for monitoring data protection;

(b) specific time limits within which data should be reviewed for erasure;

(c) measures to raise awareness of staff involved in processing operations;

(d) restrictions on access to personal data within the controller (the competent body);

(e) processing of such data using spatial and organisational separation;

(f) pseudonymisation of personal data;

(g) encryption of personal data; or

(h) specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Article 47
Processing for other purposes
(Article 4 of the Directive)

The processing of personal data for a purpose other than that for which they have been collected shall be permitted where that other purpose is one of the purposes referred to in Article 43, the controller is authorised to process data for that purpose and the processing carried out is necessary and proportionate to that other purpose. The processing of personal data for another purpose, which is not referred to in Article 43, shall be permitted where expressly provided for by law.

Article 48
Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
(Article 4 of the Directive)

Personal data may be processed in the context of the purposes referred to in Article 43 for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes, if this is in the public interest and appropriate safeguards are applied in relation to the data subject's protected legitimate rights. Such safeguards may consist in anonymising personal data as soon as possible, taking measures to prevent unauthorised third-party access or their processing using spatial and organisational separation from other specific tasks.

Article 49
Consent

1. To the extent that the processing of personal data is based on consent by law, the controller must be able to demonstrate that the data subject has given his or her consent.

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 should 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.

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 given before its withdrawal. Prior to giving consent, the data subject shall be informed of this right.

4. Consent produces its legal effects only when it is based on the data subject's free will. In assessing whether consent was freely given, account should be taken of the circumstances in which consent was given. The data subject shall be informed of the intended purpose of processing. If necessary, according to the circumstances of the case in question or upon request, the data subject shall also be informed of the consequences of the refusal of consent.

5. In case of special categories of personal data, consent must be explicitly referred to those data.

Article 50
Processing under the authority of the controller
(Article 23 of the Directive)

Any person acting under the authority of the controller or the processor, who has access to personal data, shall process such data on instructions from the controller, unless provided otherwise by law.

Article 51
Confidentiality

All persons employed in the processing of personal data shall process such data upon authorisation and shall be obliged, when taking up their duties, to maintain confidentiality. The obligation of confidentiality continues even after the termination of their employment.

Article 52
Automated individual decision-making
(Article 11 of the Directive)

1. A decision based solely on automated processing, which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be permitted only if provided for by law.

2. Decisions referred to in the previous paragraph shall not apply to special categories of personal data, unless appropriate measures to safeguard the data subject's legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

SECTION III
RIGHTS OF THE DATA SUBJECT

Article 53
General information on data processing
(Articles 12 and 13 of the Directive)

The controller shall provide general and easily accessible information to the public in plain and intelligible language through the website of the public authority with regard to:

(a) the purposes of processing,

(b) the right of the data subject to request from the controller access to, rectification, erasure or restriction of processing,

(c) the identity and the contact details of the controller and the DPO,

(d) the right to lodge a complaint with the Authority, and

(e) the contact details of the Authority.

Article 54
The data subject's right to be informed
(Article 13 of the Directive)

1. In specific cases, and in particular where the personal data of the data subject have been collected in secrecy and in order to enable the exercise of his or her rights, the data subject should, in addition to the information referred to in the previous Article, be informed, at least, of:

(a) the legal basis for the processing;

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

(c) where applicable, the recipients of the personal data;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

2. In the cases referred to in the previous paragraph, the controller may delay, restrict or omit the provision of information to the data subject, if necessary, in order to:

(a) enable the competent authorities to perform their duties, as described in Article 43,

(b) ensure national security or public security, or

(c) protect the legitimate interests of third parties, which would otherwise be threatened, if the interest in avoiding these threats overrides the interest of the data subject in being informed.

3. The provisions of paragraph 7 of the following Article shall also apply to the restrictions of the previous paragraph.

Article 55
Right of access
(Articles 14 and 15 of the Directive)

1. The controller shall, at the data subject's request, inform the data subject of the processing of personal data relating to him or her. The data subject shall also be informed of:

(a) the personal data to be processed and the categories to which they belong;

(b) any available information on the data origin;

(c) the purposes and legal basis for the processing;

(d) the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organisations;

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

(f) the possibility of exercising the right to rectification or erasure or restriction of the processing of personal data;

(g) the right to lodge a complaint with the Authority, pursuant to Article 58; and

(h) the contact details of the Authority.

2. The previous paragraph shall not apply to personal data which are processed only because they cannot be erased due to legal requirements for retention or for the sole purpose of data security or data protection audits, where the provision of information involves a disproportionate effort and the processing for other purposes through appropriate technical and organisational measures is excluded.

3. No information shall be provided if the data subject does not provide any information enabling his or her personal data to be found and, therefore, the effort involved is disproportionate to the interest of the data subject in being informed.

4. In the cases referred to in paragraph 2 of the previous Article, the controller may refuse to provide information in accordance with the first subparagraph of paragraph 1 or to restrict, in whole or in part, the provision of information in accordance with the second subparagraph of paragraph 1.

5. The data subject shall not be notified of the identity of the natural persons from whom the personal data originate, where such information is likely to endanger his or her life or physical integrity and fundamental freedoms, as well as in the case of protected witnesses or informants.

6. The controller shall inform the data subject in writing, without delay, of his or her decision to refuse or restrict access. The above notification obligation of the controller shall not apply where the provision of such information gives rise to a risk in accordance with paragraph 2 of the previous Article. The above notification shall include the factual or legal reasons on which the refusal or restriction is based, unless such justification would compromise the intended purpose of the refusal or restriction of access.

7. In case of refusal or restriction of access, the data subject, pursuant to the previous paragraph, shall be informed of the possibility of exercising the right of access through the Authority, and, in particular, the possibility of lodging a complaint with the Authority under Article 58, and of bringing an action for annulment against the Authority's negative decision before the Council of State. The decision of the controller shall be transmitted to the Authority, unless the controller invokes national security concerns. In the case of a complaint lodged with the Authority, the latter shall investigate whether the conditions necessary for the restriction of the right are met and shall inform the subject at least that all necessary verifications or reviews have been carried out by the Authority, as well as whether the provisions on the protection of personal data have been infringed.

8. The controller shall document the factual or legal reasons on which the decision is based.

Article 56

Right to rectification or erasure of personal data and restriction of processing

(Article 16 of the Directive)

1. The data subject shall have the right to obtain from the controller without delay the rectification of inaccurate personal data relating to him or her. In particular, in the case of statements or decisions, the question of accuracy is irrelevant to the content of the statement or decision. If the accuracy or inaccuracy of personal data cannot be ascertained, the controller shall restrict the processing instead of deleting the data. In such a case, the controller shall inform the data subject before resuming the restriction. The data subject may also request to have incomplete personal data completed, where this is reasonable, taking into account the purposes of the processing.

2. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without delay, where the processing of such data infringes the provisions of this Chapter, the knowledge of those data is no longer necessary for the performance of tasks or those data must be erased, so as to allow the controller to fulfil a legal obligation.

3. Instead of erasing personal data, the controller shall restrict the processing, where:

(a) there is reason to assume that the erasure would compromise the legitimate interests of the data subject,

(b) the personal data are to be kept, provided they serve as evidence for the purposes of Article 43, or

(c) erasure would be impossible or would involve a disproportionate effort due to the special storage mode.

Personal data subject to restricted processing, in accordance with the above, may be processed only for the purpose preventing their erasure.

4. In automated filing systems, technical measures should ensure that the restriction of processing is easily visible and that processing for other purposes is not possible without further examination.

5. Where the controller has rectified inaccurate personal data, he or she shall notify the rectification to the body from which the controller obtained the data. In case of rectification, erasure or restriction of processing in accordance with paragraphs 1 to 3, the controller shall inform the recipients to whom the personal data have been transmitted of those measures. The recipient shall rectify or erase the personal data or restrict their processing.

6. The controller shall inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of their processing. This shall not apply where the provision of such information gives rise to a risk in accordance with Article 54(2). The information referred to in the previous subparagraph shall include the reasons for such refusal, unless such reasons compromise the intended purpose of the refusal.

7. In other respects, paragraphs 7 and 8 of the previous Article shall apply accordingly.

Article 57

Modalities for exercising the rights of the data subject

(Article 12 of the Directive)

1. The controller shall communicate with the data subject in a concise, intelligible and easily accessible form, using clear and plain language, in particular when addressing minors. The information shall be provided without prejudice to specific provisions by any appropriate means, including by electronic means. The controller should provide the information in the same form as the request.

2. Without prejudice to Article 55(5) and Article 56(6), the controller shall without delay inform the data subject of the

status of his or her request.

3. The information provided in accordance with Article 53, any communication made in accordance with Articles 54 and 64, as well as the requests processed in accordance with Articles 55 and 56, shall not be subject to a fee. Where a request in accordance with Articles 55 and 56 is manifestly unfounded or is being abused, the controller may charge a reasonable fee based on administrative costs or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request.

4. Where the controller has reasonable doubts concerning the identity of the data subject making the request referred to in Articles 55 and 56, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 58
Right to lodge a complaint with the Authority
(Article 17 of the Directive)

1. The data subject shall have the right to lodge a complaint with the Authority, if the data subject considers that the processing of personal data relating to him or her by public authorities for the purposes referred to in Article 43 infringes his or her rights. This shall not apply to the processing of personal data by the judicial and prosecutorial authorities when processing such data acting in their judicial capacity. The Authority shall inform the data subject of the progress and the outcome of the complaint and of the possibility of bringing an action for annulment before the Council of State against the decision on his or her complaint, in accordance with Article 20.

2. Where a complaint relating to processing is lodged with the Authority instead of the competent supervisory authority of another Member State of the European Union, the Authority should transmit without delay to the supervisory authority of the other Member State of the European Union the complaint falling within its competence. In such a case, the Authority shall inform the data subject of the transmission of his or her complaint and provide him or her with any assistance upon his or her request.

Article 59
Rights of the data subject in criminal investigations and proceedings
(Article 18 of the Directive)

In the context of criminal investigations and proceedings, the right to be informed of the processing, to access, rectification or erasure and restriction of personal data, in accordance with the provisions of Articles 54 to 56, shall be exercised in accordance with the provisions of the Code of Criminal Procedure, specific procedural provisions and the Code of court organisation and status of judicial officials, as applicable each time.

SECTION IV
OBLIGATIONS OF PROCESSORS AND CONTROLLERS

Article 60
Processor
(Articles 22 and 23 of the Directive)

1. Where processing is carried out on behalf of a controller, the controller shall ensure compliance with the obligations arising from this Law and other provisions relating to the protection of personal data. The right of the data subject to be informed, to rectification, erasure and restriction of the processing of personal data, as well as the right to compensation in this case shall be exercised vis-à-vis the controller.

2. The controller shall be allowed to assign the processing of personal data only to processors who ensure that, by implementing appropriate technical and organisational measures, processing is carried out in accordance with the law and that the protection of the rights of the data subject is guaranteed.

3. The carrying out of processing by a processor should be governed by a contract or other legal act binding the processor to the controller and that sets out the subject matter, duration, nature and purpose of the processing, the categories of data subjects and the rights and obligations of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) acts only on instructions from the controller; where the processor is of the opinion that an instruction is unlawful, the processor should inform the controller without delay;

(b) guarantees that persons authorised to process the personal data have pledged themselves to confidentiality to the extent that they are not under a valid statutory obligation of confidentiality;

(c) assists the controller by any appropriate means to safeguard the data subject's rights;

(d) at the controller's discretion, returns or deletes all the personal data after the end of the provision of data processing services, and deletes existing copies, unless there is a legal obligation to store the data;

(e) provides to the controller all information necessary to demonstrate compliance with his or her obligations, in particular logs created in accordance with Article 74;

(f) allows audits to be carried out by the controller or the auditor authorised by the controller, and contributes to such audits;

(g) takes all necessary measures in accordance with Article 62;

(h) taking into account the nature of the processing and the information available, assists the controller to ensure compliance with the obligations laid down in Articles 62 to 65 and 67.

4. In the event that the processor engages another processor, the processor should impose the same obligations laid down in the contract with the controller, in accordance with paragraph 3, which also applies to the processor, unless these obligations are already binding on the other processor under other provisions.

5. The processor may engage another processor only with prior written authorisation from the controller. Where the controller has given general authorisation to the processor for the participation of another processor, 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.

6. The contract referred to in paragraph 3 shall be in writing or in electronic form.

7. A processor who determines, in infringement of this Article, the purposes and means of processing shall be considered to be a controller.

Article 61
Joint controllers
(Article 21 of the Directive)

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. The duties and responsibilities of each joint controller shall be determined in a transparent manner, by means of a written arrangement, to the extent that their duties and responsibilities are not determined by law. In particular, the arrangement shall designate the person who will be responsible for meeting the information obligations and before which authority the data subjects may exercise their rights.

2. The terms of the arrangement referred to in the previous paragraph shall not prevent the data subject from exercising his or her rights against each of the joint controllers.

Article 62
Security of processing
(Articles 19 and 29 of the Directive)

1. The controller and processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risks involved by the processing for the data subjects, shall take the necessary technical and organisational measures to ensure a level of security appropriate to the risk during the processing of personal data, in particular as regards the processing of special categories of personal data.

2. The measures referred to in the previous paragraph may include, inter alia, the pseudonymisation and encryption of personal data, where such measures are possible for the purposes of the processing. The measures in accordance with paragraph 1 should ensure:

(a) the confidentiality, integrity, availability and resilience of processing systems and services; and

(b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

3. In respect of automated processing, the controller and processor, following an evaluation of the risks, shall implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems, and when and by whom the personal data were input ('input control');

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity');

(k) ensure that the personal data to be processed on behalf of the controller can only be processed according to the instructions of the controller ('processing control');

(l) ensure that the personal data are protected from loss and destruction (availability control);

(m) ensure that the personal data collected for different purposes can be processed using organisational or spatial separation (possibility of separation).

The purpose of the first subparagraph in indents (b) to (e) may be achieved, in particular, by means of encryption technology.

Article 63
Notification of a personal data breach to the Authority
(Article 30 of the Directive)

1. In the case of a personal data breach, the controller shall notify without delay and, where feasible, not later than seventy two (72) hours after having become aware of it, the personal data breach to the Authority, unless he or she reasonably considers on the basis of justifiable reasons that the breach is not likely to compromise the protected legal interests of a natural person. The notification of the breach to the Authority after the expiry of seventy two (72) hours shall be specifically justified as regards the reasons for the delay.

2. The processor shall notify the controller without delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall contain at least the following information:

(a) the nature of the personal data breach including, where possible, the categories and number of data subjects concerned, and the categories and number of personal

data records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) a description of the likely consequences of the personal data breach; and

(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach and to mitigate its possible adverse effects.

4. Where it is not possible to provide the information referred to in the previous paragraph at the same time with the notification of the breach, the controller may provide the information in phases once it is available without further delay.

5. The controller shall document any personal data breach comprising of the facts relating to the personal data breach, its effects and the remedial action taken.

6. Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in paragraph 3 shall be communicated to the controller of that Member State without delay.

7. Further obligations of the controller regarding the notification of personal data breaches shall remain unaffected.

Article 64
Communication of a personal data breach to the data subject
(Article 31 of the Directive)

1. Where the personal data breach is likely to result in a significant risk to the protected legitimate interests of a natural person, the controller shall communicate the personal data breach to the data subject without delay.

2. When notifying the data subject in accordance with paragraph 1, the nature of the personal data breach shall be described in clear and plain language and the content of points (b), (c) and (d) of paragraph 3 of the previous Article shall be at least indicated.

3. A communication to the data subject shall not be required if any of the following conditions are met:

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

(b) the controller has taken subsequent measures which ensure protection against personal data breach; or

(c) disproportionate efforts are required. In such a case, there shall instead be a public communication or similar measures whereby the data subjects are informed in an equally effective manner.

4. If the controller has not informed the data subject of the personal data breach, the Authority may formally declare that it considers that the conditions of paragraph 3 are not met. In doing so, it should consider the likelihood that the damage will result in a significant risk within the meaning of paragraph 1.

5. The communication to the data subject pursuant to paragraph 1 may be delayed, restricted or omitted subject to the conditions laid down in Article 54(2), except where the interests of the data subject override the significant risk of the breach within the meaning of paragraph 1.

Article 65
Assessment of the impact of processing on the protection of personal data
(Article 27 of the Directive)

1. If a form of processing, in particular where using new technologies, is likely to result in a significant risk to the protected legitimate interests of the data subjects due to the nature, scope, conditions and purposes of the processing, the controller shall first carry out an assessment of the impact of the envisaged processing for the data subjects.

2. To investigate such processing operations with similar potential for significant risk, a data protection impact assessment may be carried out jointly.

3. The impact assessment shall take into account the rights of the data subject which are affected by the processing and must contain at least the following:

(a) a systematic description of the envisaged operations and purposes of the processing;

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

(c) an assessment of the risks to the protected legitimate interests of the data subject; and

d) the measures to be taken to address the existing risks, including safeguards, security measures and procedures to ensure the protection of personal data and to demonstrate compliance with legal requirements.

4. Where necessary, the controller shall check whether the processing complies with the requirements of the impact assessment.

Article 66
Cooperation with the Authority
(Article 26 of the Directive)

The controller and processor shall cooperate with the Authority in the performance of its tasks.

Article 67
Prior consultation of the Authority
(Article 28 of the Directive)

1. The controller shall consult the Authority prior to processing personal data which will form part of a new filing system to be created, where:

(a) a data protection impact assessment as provided for in Article 65 indicates that the processing would result in a significant risk to the protected legitimate interests of the data subject in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular due to the use of new technologies, mechanisms or procedures, involves a significant risk to the protected legitimate interests of the data subject.

2. During the preparation of draft laws or regulations relating to the processing of personal data by competent authorities for the purposes of Article 43 or linked to the processing, the Authority shall be consulted in a timely manner.

3. The Authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1. The Authority shall communicate this list to the controller.

4. During prior consultation, the Authority shall be provided with:

(a) a data protection impact assessment carried out in accordance with Article 65;

(b) where applicable, information about the responsibilities of the controller, joint controllers and processors involved;

(c) information about the purposes and means of the intended processing;

(d) information about the measures and safeguards provided to protect the legitimate interests of the data subjects; and

(e) the name and contact details of the DPO.

The Authority shall receive upon request any other information necessary to assess the lawfulness of the processing and, in particular, the existing risks for the protection of personal data of the data subjects and of the related safeguards.

5. Where the Authority is of the opinion that the intended processing would infringe the law, in particular where the controller has insufficiently identified the risk or has not taken sufficient measures to mitigate the risk, the Authority may provide, within a period of up to six (6) weeks of receipt of the request for consultation, written recommendations to the controller and, where applicable, the processor with regard to additional measures to be taken. The Authority may extend that period by one (1) month if the intended processing is highly complex. In this case, the Authority shall inform the controller or processor of any such extension.

6. Where the envisaged processing is necessary for the performance of the tasks of the controller, and is therefore particularly urgent, the controller may initiate such processing after the start of the consultation, but before the expiry of the period referred to in the first subparagraph of the previous paragraph. In this case, the recommendations must be taken into account ex post and the method of processing shall be adjusted accordingly.

Article 68
Records of processing activities
(Article 24 of the Directive)

1. The controller shall maintain a record of all categories of processing activities under his or her responsibility. That record shall contain the following information:

(a) the name or business name and the contact details of the controller and, where applicable, any joint controller and the DPO;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;

(d) a description of the categories of data subjects and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(g) an indication of the legal basis for the processing;

(h) the prescribed time limits for erasure of the different categories of personal data or for review of the need for their erasure; and

(i) a general description of the technical and organisational security measures referred to in Article 62.

2. The processor should maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name or business name and the contact details of each processor, each controller on behalf of whom the processor is acting and, where applicable, of the DPO;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to an identified third country or an international organisation where the processor has explicitly been instructed to do so by the controller; and

(d) where possible, a general description of the technical and organisational security measures referred to in Article 62.

3. The records referred to in paragraphs 1 and 2 shall be in writing.

4. The controller and processor shall make those records available to the Authority on request.

Article 69
Data protection by design and by default
(Article 20 of the Directive)

1. The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, take appropriate measures to implement data protection principles, such as data minimisation, in an effective manner, in order to ensure compliance with the legal requirements and the protection of the rights of data subjects. The controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the protected legitimate interests of the data subject. In particular, personal data shall be processed and the processing systems shall be selected and designed in accordance with the principle of minimisation. As far as possible, personal data shall be anonymised or pseudonymised as soon as possible in accordance with the purpose of the processing.

2. The controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. This 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 by automated means to an indefinite number of persons.

Article 70
Distinction between different categories of data subject
(Article 6 of the Directive)

1. Where processing personal data, the controller shall, as far as possible, make a clear distinction between different categories of data subjects. This applies in particular to the following categories:

(a) persons with regard to whom there are serious grounds for believing that they have committed a criminal offence;

(b) persons with regard to whom there are serious grounds for believing that they are about to commit a criminal offence;

(c) persons convicted of a criminal offence;

(d) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(e) other persons, such as witnesses, informants or contacts or associates of the persons referred to in indents (a) to (d).

Article 71
Distinction between personal data and verification of their identity
(Article 7 of the Directive)

During processing, the controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments. To this end, the controller shall specify the evaluations based on personal assessments as such, insofar as it is feasible, in the context of such processing. It should also be possible to determine which public authority maintains the records on which the evaluation upon personal assessment is based.

Article 72
Transmission procedure
(Articles 7 and 9 of the Directive)

1. The controller shall take appropriate measures to ensure that personal data which are inaccurate or no longer up to date are not transmitted or otherwise made available. To that end, the controller shall, as far as possible, verify the quality of personal data before they are transmitted or made available, making a reasonable effort. The controller should also, as far as possible and reasonable, in all transmissions of personal data include necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date.

2. Where the processing of personal data is subject to specific conditions as to the transmission of data, the transmitting authority shall inform the recipient of those conditions and the requirement to comply with them. The obligation to provide information may be fulfilled by marking the data accordingly.

3. The transmitting competent authority shall not apply the conditions set out in the previous paragraph to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the within the Greek territory.

Article 73
Rectification and erasure of personal data and restriction of processing
(Article 5 of the Directive)

1. The controller shall rectify inaccurate personal data.

2. The controller shall erase personal data without delay, if the processing is unlawful, and the data must be erased to comply with a legal obligation or it is no longer necessary for the controller to be aware of such data to perform his or her tasks.

3. Paragraphs 3 to 5 of Article 56 shall apply accordingly. The recipient shall also be informed whether or not inaccurate personal data have been transmitted or whether personal data have been transmitted unlawfully.

4. Without prejudice to the maximum time limits for storage or erasure laid down in legal provisions, the controller shall provide for the erasure of personal data or for a periodic review of the need for storing personal data and shall ensure compliance with those time limits based on set procedural regulations.

Article 74
Logging
(Article 25 of the Directive)

1. The controller and the processor shall keep logs in automated processing systems for at least the following processing operations:

(a) collection,

(b) alteration,

(c) consultation,

(d) disclosure including transfers;

(e) combination and

(f) erasure.

2. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

3. The logs shall be used solely for verification of the lawfulness of data processing by the Authority and the data subject, as well as for self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

4. The logs shall be deleted at the end of the year following the year in which they were created.

5. The controller and processor shall make the logs available to the Authority on request.

SECTION V
TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 75
General principles for transfers of personal data
(Article 35 of the Directive)

1. Where all the other conditions for transfers of personal data laid down in this Chapter are met, the transfer of personal data to the authorities of third countries or international organisations may take place, where:

(a) the authority or international organisation is competent for the purposes referred to in Article 43, and

(b) the Commission has adopted a decision ensuring an adequate level of protection in the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to the following Article or, in the absence of the above, derogations for specific situations apply pursuant to Article 77.

2. The transfer of personal data may not take place, in spite of an adequacy decision in accordance with the previous paragraph and although this is required by the public interest, if, in such case, the protection of the data subject's fundamental rights and legitimate interests cannot be ensured when their data are processed by their recipient. The controller shall assess the level of protection of such rights and legitimate interests of the data subject on the basis of whether the recipient of the personal data in the third country ensures in this case their appropriate protection.

3. Where personal data transferred or made available from another Member State of the European Union must be transferred in accordance with paragraph 1, the competent authority of the other Member State must have first given its authorisation to such transfer. Transfers without prior authorisation shall be permitted only where the transfer is necessary for the prevention of an immediate and serious risk to public security of a State or to essential interests of a Member State and the prior authorisation cannot be obtained in a timely manner. In the case of paragraph 2, the authority or body of the other Member State responsible for giving authorisation shall be informed of the transfer immediately.

4. The controller transferring personal data pursuant to paragraph 1 shall take appropriate measures to ensure that the recipient transmits only the data transmitted to other third countries or international organisations, where the controller has given prior authorisation to such transfer. Where the controller decides to give authorisation, the controller shall take due account of all relevant factors, in particular the seriousness of the offence, the purpose for which the data were originally transferred, and the level of personal data protection in the third country or international organisation to which personal data are to be transferred. An authorisation may be given only if it is permitted to transfer personal data directly to another third country or international organisation.

Article 76
Transfers subject to appropriate safeguards
(Article 37 of the Directive)

1. In the absence of an adequacy decision pursuant to subparagraph (b) of paragraph 1 of the previous Article, a transfer of personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument, or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall record the transfers under indent (b) of paragraph 1. The recording shall include the date and time of the transfer, the identity of the recipient, the justification for the transfer and the personal data transferred. The above recording shall be made available to the Authority upon request.

Article 77
Derogations for specific situations
(Article 38 of the Directive)

1. In the absence of an adequacy decision pursuant to Article 75(1)(b), or of appropriate safeguards pursuant to paragraph 1 of the previous Article, transfers meeting the other conditions of Article 75 may take place only on the condition that this is necessary in order to:

(a) protect the vital interests of the data subject or another person,

(b) safeguard legitimate interests of the data subject,

(c) prevent an immediate and serious threat to public security of a country,

(d) in individual cases for the purposes set out in Article 43, or

(e) in individual cases for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 43.

2. The transfer of personal data pursuant to the previous paragraph shall not be permitted, where the transferring competent authority determines that the data subject's fundamental rights and legitimate interests override the public interest in the transfer.

3. Paragraph 2 of the previous Article shall apply accordingly to the transfers referred to in paragraph 1.

Article 78
Transfers of personal data to recipients established in third countries
(Article 39 of the Directive)

1. In specific individual cases, and if all other requirements for data transfers to third countries are fulfilled, controllers may transfer personal data directly to recipients established in third countries not referred to in indent (a) of Article 75(1), if the transfer is strictly necessary for the performance of their tasks, and

(a) in this case, no fundamental right of the data subject overrides the public interest necessitating the transfer,

(b) the transfer to the authorities referred to in in Article 75(1)(a) is ineffective or inappropriate, in particular because the transfer cannot be achieved in a timely manner, and

(c) the controller informs the recipient of the purposes of the processing and gives clear instructions to the recipient that the transmitted data may be processed only to the extent necessary for such purposes.

2. In the case of paragraph 1, the controller shall inform without delay the authorities referred to in indent (a) of Article 75(1), unless that is ineffective or inappropriate.

3. Paragraphs 2 and 3 of Article 75 shall apply accordingly to transfers in accordance with paragraph 1.

4. In the case of transfers referred to in paragraph 1, the controller shall oblige the recipient to process the personal data transferred without the consent of the controller only for the purpose for which the data were transmitted.

5. Agreements in the field of judicial cooperation in criminal matters and police cooperation shall remain unaffected.

SECTION VI
COOPERATION BETWEEN SUPERVISORY AUTHORITIES

Article 79
Mutual assistance
(Article 50 of the Directive)

1. The Authority shall provide the supervisory authorities of other Member States with information and mutual assistance insofar as necessary in order to implement this Chapter. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

2. The Authority shall take all appropriate measures required to reply to a request of another supervisory authority for mutual assistance without delay and no later than one month after receiving the request.

3. The Authority may refuse to comply with the request:

(a) if it is not competent for the subject matter of the request or for the measures it is requested to execute, or

(b) compliance with the request infringes the law.

4. The Authority shall inform the requesting supervisory authority of the other Member State of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In the case of the previous paragraph, it shall justify its refusal to comply with the request.

5. The Authority shall, as a rule, supply the information requested by the supervisory authority of the other Member State by electronic means and in a standardised format.

6. The Authority shall not charge a fee for actions taken pursuant to a request for mutual assistance, unless it has agreed with the supervisory authority of the other State to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

7. Requests to the Authority for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

SECTION VII
LIABILITY AND PENALTIES

Article 80
Liability of the controller
(Articles 54 and 56 of the Directive)

A public authority, in its capacity as a controller, having unlawfully caused damage to the data subject, in breach of the provisions of Articles 6 to 8 or the provisions of this Chapter, shall be required, in accordance with the provisions of Articles 105 and 106 of the Introductory Law to the Greek Civil Code, to pay compensation or damages for non-material damage to the data subject.

Article 81
Criminal penalties
(Articles 54 and 57 of the Directive)

Article 38 shall also apply to the processing of personal data by competent authorities for the purposes of Article 43.

Article 82
Administrative penalties
(Articles 54 and 57 of the Directive)

1. Without prejudice to the supervisory powers of the Authority pursuant to Article 15 of this Law, the Authority, in a specific reasoned decision and following a previous notice summoning the interested parties to provide explanations, may impose the following administrative fines on competent authorities for infringements of their obligations as data controllers:

(a) for infringements of Articles 6 to 8 and Articles 60 to 78, an administrative fine of up to one million euros (EUR 1,000,000),

(b) for infringements of Articles 45 to 57, an administrative fine up to two million euros (EUR 2,000,000) and

(c) for failure to comply with an order of the Authority under Article 15(4), an administrative fine of up to two million euros (EUR 2,000,000).

2. When deciding whether to impose an administrative fine and determining its amount, in each individual case due regard shall be given to the following:

(a) the nature, gravity, duration of the infringement, scope or purpose of the processing concerned and the number of data subjects affected by the breach and the extent of the damage suffered,

(b) any actions taken by the competent authority to mitigate the damage suffered by the data subjects,

(c) any relevant previous infringements by the competent authority,

(d) the categories of personal data affected by the infringement,

(e) the manner in which the infringement became known to the Authority, in particular whether, and if so to what extent, the competent authority notified the infringement and

(f) in case the measures referred to in Article 15(4) have already been ordered against the competent authority with regard to the same infringement, the degree of compliance with those measures.

CHAPTER E
FINAL AND TRANSITIONAL PROVISIONS

Article 83
Transitional provisions

1. Reference to Law 2472/1997 made in provisions of the legislation in force shall be construed as reference to the relevant provisions of the GDPR and of this Law.

2. The guidelines and regulatory acts of the Authority shall remain in force, provided that they do not infringe the GDPR and the provisions of this Law.

3. The staff serving at the Authority at the time of passing this Law, both permanent and under an employment relationship governed by private law, shall be automatically assigned to equivalent positions governed by public or private law for each category, branch or specialty, in accordance with their formal qualifications.

4. Requests pending before the Authority until 25.5.2018 will be filed without further action following a declaratory act of the President with the exception of data subjects’ admissible applications.

Article 84
Repealed provisions

Law 2472/1997 on the protection of individuals with regard to the processing of personal data shall be repealed, without prejudice to the definitions of Article 2, where explicit reference is made to those definitions in legislation on personal data, to indent (b) of Article 2 (from the second until the last subparagraph) regarding the notification and disclosure of personal data and to subparagraph (b) of Article 3(2) only with regard to the offences described therein, to indent (b) of Article 3(2) of the above law (from the third until the last subparagraph) on the establishment and operation of surveillance systems, to Article 13(3), Article 15(3) regarding the establishment of the Authority, to Article 18(2) and (3) and to Article 21 on the imposition of administrative sanctions under Article 13(4) of Law 3471/2006 (Government Gazette A’ 133), which remain in force.

Article 85
Validity of international or bilateral international agreements

International or bilateral international agreements relating to the transfer of personal data to third countries or international organisations in the area of judicial cooperation in criminal matters or police cooperation concluded before 6.5.2016, which comply with the Union law applicable prior to that date, shall remain in force until amended, replaced or revoked.

* Article 86
* [This article is irrelevant to the data protection legislation. It is an amendment to another, unrelated act of law.]

1. As from the entry into force of this Law, and without prejudice to paragraphs 2, 3 and 4, the following shall be repealed: (a) Article 1 of the Legislative Act of 18.7.2015 “Urgent provisions for imposing restrictions on cash withdrawals and capital transfers” (Government Gazette A’ 84,), which was ratified by Article 4 of Law 4350/2015 (Government Gazette A’ 161), as in force; (b) the ministerial orders adopted pursuant to authorisation provided by the above Legislative Act of 18.7.2015; and (c) the regulatory decisions of the Banking Transactions Approval Committee, which was set up in accordance with paragraph 4 of the first Article of the Legislative Act of 28 June 2015 “Short-term bank holiday” (Government Gazette A’ 65) ratified by Article 1 of Law 4350/2015, as in force.

2. The Bank of Greece and the Hellenic Capital Market Commission shall remain responsible for the continuation of outstanding audits and the conduct of new audits (sample or following a complaint) on the compliance of the institutions and bodies they supervise with the provisions of the Legislative Act of 18.7.2015 “Urgent provisions for imposing restrictions on cash withdrawals and capital transfers” (Government Gazette A’ 84) ratified by Article 4 of Law 4350/2015 (Government Gazette A’ 161), as in force, for infringements of its provisions which have taken place until the entry into force of this Law. Paragraphs 13 and 13a of the first Article of the Legislative Act of 18.7.2015 “Urgent provisions for imposing restrictions on cash withdrawals and capital transfers” (Government Gazette A’ 84) ratified by Article 4 of Law 4350/2015 (Government Gazette A’ 161), as in force, shall remain in force.

3. Paragraph 14 of the first Article of the Legislative Act of 18.7.2015 “Urgent provisions for imposing restrictions on cash withdrawals and capital transfers” (Government Gazette A’ 84) ratified by Article 4 of Law 4350/2015 (Government Gazette A’ 161), as in force, shall remain in force for infringements of its provisions which have taken place until the entry into force of this Law.

4. The first and second subparagraphs of paragraph 15 of the first Article of the Legislative Act of 18.7.2015 “‘Urgent provisions for imposing restrictions on cash withdrawals and capital transfers” (Government Gazette A’ 84) ratified by Article 4 of Law 4350/2015 (Government Gazette A’ 161), as in force, shall remain in force.

5. The electronic file of the Banking Transactions Approval Committee shall be sealed and remain unaltered, in dormant state, in the relevant systems of the Bank of Greece under the responsibility of the Bank’s Information Systems Department. In particular, matters relating to the electronic file may be dealt with by means of an act of the Bank of Greece Governor. The physical file shall be kept at the Financial Policy Division of the General Secretariat of Economic Policy of the Ministry of Finance. Specific matters relating to the natural file may be dealt with by decision of the Minister of Finance. The file shall be accessible to the supervisory authorities referred to in paragraph 2, as well as to any supervisory, judicial or prosecutorial authority to enable them to investigate acts or omissions related to infringements of the repealed provisions of paragraph 1 during the period of validity of such provisions. Information contained in the file may be deleted by decision of the Minister of Finance after a period of 20 years from the date on which the decision of the Banking Transactions Approval Committee was adopted.

6. This Law shall enter into force on 1.9.2019.

Article 87
Entry into force

This Law shall enter into force on the date of its publication in the Government Gazette, unless otherwise provided for in other provisions.

We hereby order the publication of this Law in the Government Gazette and its execution as law of the State.

Athens, 28 August 2019
The President of the Republic
PROKOPIOS V. PAVLOPOULOS

The Ministers
of Finance of Justice
CHRISTOS STAIKOURAS **KONSTANTINOS TSIARAS**

Authenticated and stamped with the Great Seal of the State.

Athens, 29 August 2019
The Minister of Justice
KONSTANTINOS TSIARAS