2019

Problem based training on the data protection reform package in GR and CY – TRAIN-GR-CY

769169 — TRAIN-GR-CY — REC-DATA-2016/REC-DATA-2016-01

MODEL CODE OF PRACTICE

TO FACILITATE COMPLIANCE WITH THE LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA

This document was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020). The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

MODEL CODE OF PRACTICE

TO FACILITATE COMPLIANCE WITH THE LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA

Introductory note

This Model was elaborated on behalf of the Centre for European Constitutional Law – Themistokles and Dimitris Tsatsos Foundation, as part of the project 'PROBLEM BASED TRAINING ON THE DATA PROTECTION REFORM PACKAGE IN GR AND CY — TRAIN-GR-CY'.

Since the design phase of the project, a Model Code of Practice was foreseen as one of its deliverables. During the project's implementation phase, it was firmly established that drafting Codes of Practice, as practical Guides, for a particular activity and taking into account its specificities, can greatly facilitate the efforts to comply with the framework for data protection.

Moreover, it was noted that Codes of Practice should always entail basic information on the current legal framework (Regulation (EU) 2016/679 and national legislation), on the one hand, and specific issues to be taken into consideration, as well as practical guidance/directions to properly address the main issues that arise, depending on the specificities of the activity concerned, on the other.

As indicated above, Codes of Practice can cover a specific activity, on a horizontal or a vertical basis. As such, they may relate to a specific group of professionals, covering the entire range of their activity and all its aspects that entail personal data processing (for example, Code of Practice for lawyers or notaries). They may also relate to Data Protection Officers in general, or those engaged in specific activities in particular (for example, Code of Practice for Data Protection Officers engaged in insurance undertakings). Moreover, they may only concern a large public sector organization – in which case using a Code of Conduct is not possible – or a large private sector company. The possibility of drafting a Code of Practice for smaller-scale users is of course not excluded.

The following Model Code of Practice was elaborated in the context of the aforementioned project. It aims to serve as a model for different Codes of Practice, in terms of structure, as mentioned above. The main objective was to develop a standard form that can be generally utilized to the extent possible. Substantive provisions are added on a case-by-case basis and only for

illustrative purposes, in order to better understand the scope of the respective field of activity. The examples are mostly related to practicing law, given the fact that the program's participants are more familiar with it. As such, it is easier for them to understand the Code's structure and the objectives pursued.

Recommendations on good practices are included in some parts of the draft Code (under the title "Recommendations"), taking into consideration that the Code should encompass specific recommendations concerning crucial aspects of each activity.

All project partners (The Centre for European Constitutional Law, the Greek Data Protection Authority, The University of Cyprus, the Laboratory of Law and Informatics National and Kapodistrian University of Athens Law School, the Office of the Commissioner for Personal Data Protection) participated in the development of this Model Code of Practice. Special mention should be made to Ms Irene Loizidou Nikolaidou, Commissioner for personal data protection in Cyprus, for her valuable contribution in relation to the Cypriot framework. A number of participants to the project's activities also participated in the development of the Code. These are professionals working in the three target groups of the project (judges, lawyers, DPOs). Special thanks are due to P. Bourletidou, A. Christoforou, A. Kareklas, X. Kasapi, D. Kolios, Ch. Kotios, P. Syrigos, K. Toumbanou and E. Vrakatseli. Panagiotis Perakis, lawyer and member of the Foundation's Scientific Council, drew up the present Model, based on the drafts, recommendations and observations of the aforementioned working groups.

Moreover, the Model Code was based on documents relating to the activity concerned (practicing law), which served as examples, such as the "Guide (Manual) for the Implementation of the General Data Protection Regulation (GDPR) in Legal Practice", drafted by the Laboratory of Law and Informatics of the National and Kapodistrian University of Athens Law School (authors: L. Mitrou, G. Giannopoulos, F. Panagopoulou, A. Varveris) on behalf of the Athens Bar Association, the draft "Code of Conduct for processing personal data by Lawyers/Law Firms", and other relevant documents ("Guides") by other states.

Finally, it is noted that the chapter on Data Protection Officers is more

extensive than the others. The work carried out by the respective working group was utilized, considering that it could be useful in any case. However, this does not necessarily mean that the whole chapter should always be maintained to its full extent.

TABLE OF CONTENTS

NOTE

- This Code is an informal Guide, which aims to facilitate the fulfilment of the obligations imposed by the aforementioned legal framework.
- This Code is not to be considered a Code of Conduct, foreseen by article 40 of Regulation (EU) 2016/679.
- This Code's scope covers only a number of the issues that are regulated by the legislation.
- In case that the provisions of the Code are ambiguous or inconsistent with the provisions of the law, the latter prevail.
- Compliance with this Code is without prejudice to the obligations imposed by the aforementioned Regulation and the relevant national law.

PART A

Before the implementation of the Code

Recommendations:

- Before drafting and finalizing the Code, search for already existing Codes, Guides, or even Codes of Conduct, relevant to the activity concerned, in the same or other states where Regulation (EU) 2016/679 (hereinafter referred to as "GDPR" or "the Regulation") is applicable. Compliance is facilitated by the utilization of prior experience and by uniform practice.
- Consult with stakeholders (for example, the legal community) by means of publishing a draft Code and gathering comments and feedback. Follow the same process when the Code is updated.
- Send the Code to the national Data Protection Authority for comments, after it has been finalized and the aforementioned steps have been completed and before its implementation. Follow the same process when the Code is updated, taking into consideration the number of changes and whether they are substantial.

PART B

Main part

Key features of the legal framework and implementation

1. Introduction

The General Data Protection Regulation (EU) 2016/679 became applicable on 25 May 2018. The Regulation's scope is very wide and it covers both the private and the public sector.

The Regulation applies to the processing of personal data wholly or partly by automated means, namely of any information relating to an identified or identifiable natural (living) person. It also applies to processing other than by automated means of personal data which form part or are intended to form part of a filing system.

As mentioned above, this Code does not apply to the processing of personal data of deceased persons. However, if such data may identify or correlate to the personal data of an identified or identifiable living person, they should be considered and treated as this (living) person's personal data.

After the Regulation became applicable, Law 4624/2019 was adopted in Greece. The law regulates issues that the Regulation left to the discretion of the domestic legislator.

The main domestic law for the protection of personal data in Greece was previously Law 2472/1997, which established the Hellenic Data Protection Authority. The latter was maintained as the supervisory body for the protection of personal data in Greece, within the meaning of the Regulation.

In Cyprus, the main law is Law 125(I)/2018, while the Office of the Commissioner for Personal Data Protection is the National Data Protection Authority.

2. Basic definitions

The following terms are defined as follows, as per the legal framework mentioned above:

1. **"Personal data"**: any information relating to an (already) identified or identifiable natural person ("data subject").
2. **"Identifiable natural person"**: a person 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.
3. **"Special categories of personal data"**: data which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, processing of genetic or biometric data allowing the unique identification of a person, data concerning health or data concerning sex life or sexual orientation of a person, as well as data concerning criminal offences and convictions which constitute a special category.
4. **"Processing"**: 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
5. **"Filing system"**: any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
6. **"Recipient"**: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether

a third party or not.

7. **"Data concerning health"**: 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.

8. **"Biometric data"**: 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.

9. **"Genetic data"**: 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.

10. **"Personal data relating to criminal offences and convictions"**: data relating to criminal prosecutions, including preliminary examinations, criminal procedures, convictions and security measures.

11. **"Controller"**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

12. **"Processor"**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

13. **"Third party"**: a natural or legal person, public authority, agency

or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorized to process personal data.

14. **"Consent"** of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which she or he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to her or him.

15. **"Pseudonymization"**: 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

16. **"Profiling"**: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

17. **"Personal data breach"**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Specific definitions

Add here the legal definitions of key concepts relating to the specific field of application of your Code, as defined in the relevant regulatory framework. For example, in a case where the Code is to be applied to lawyers in Greece:

- **"Law firm":** a civil law professional partnership established by practicing lawyers, as per article 49 of the Greek Code of Lawyers.
- **"Lawyer":** a person that has acquired the status of a lawyer, as per article 4 of the Greek Code of Lawyers.
- **"Mandate":** a private law relationship between a lawyer/law firm and a client for the latter's representation and defence before any court, authority, agency or extra-judicial institution, legal consultation and provision of legal advice and opinions or the undertaking of a task provided for or permitted by the Lawyers' Code, etc.

4. Basic principles

The legal framework for the protection of personal data provides for and requires that the principles mentioned below are always respected.

A central feature of the institutional framework is that the controller, as well as the processor, shall be able to demonstrate, at any given moment, that each processing of personal data is in compliance with the Regulation and any additional or specific provisions of the national legislation and that she/he has taken all the necessary measures to that end, in accordance with the **accountability principle**.

As such, continuous and prompt documentation of each action undertaken in compliance with the legal framework is necessary. The burden falls on the person to whom the task of monitoring compliance with the Code has been entrusted (see below).

Without prejudice to the fundamental principle of **proportionality**, as well, which inter alia requires the choice of the least restrictive measure for the subject (in other words, the least threatening solution with regard to her/his rights), a series of basic principles relating to data protection are introduced by the applicable legal framework.

According to these, personal data shall be:

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**).
- processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness and transparency**).
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimization**).
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**).
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (**storage limitation**).
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (**integrity and confidentiality**).

Examples of application of the aforementioned principles to the activity concerned:

Add here specific provisions relating to the application of the aforementioned principles to the everyday practice of the activity regulated by the Code. For example, in the case of legal practice:

Regarding fair and lawful collection, the principles of proportionality and data minimization:

- Lawyers/Law firms shall ensure that only data that are adequate, relevant and limited to what is necessary in relation to the purposes

of the processing in question are processed.

- Lawyers/Law firms shall process personal data only if and in so far as the processing is necessary to establish, exercise or defend legal claims (in particular) before courts, administrative or disciplinary bodies, as well as for the execution and within the mandate granted by their clients in general. They shall not use, invoke or in general process personal data which – regardless of their accuracy/truth – are not relevant to the subject-matter of the trial and/or the case in question.
- Lawyers/Law firms shall access, collect and process personal data of a third party provided that such data are derived from either publicly accessible sources/authorities or legal files maintained by judicial or other public authorities.
- Lawyers/Law firms shall ensure that they use, invoke and in general process as evidence personal data, collected fairly and lawfully, in compliance with the rules, guarantees and procedures prescribed by law.
- Lawyers/Law firms shall use, invoke and in general process as evidence personal data, which are appropriate and necessary to support their clients' claims, rights and pleas.
- Lawyers/Law firms shall undertake not to use personal data contained in documents, evidence etc., which are included in a different case file, without prior information to and [consent of] the data subjects.
- Lawyers/Law firms shall undertake to refrain from invoking or reporting personal data for the purposes of creating [negative] impressions of the data subjects or for showmanship.
- Lawyers/Law firms may use, invoke or in general use personal data, which are necessary to assess the credibility of the claims and evidence invoked by the parties, witnesses and in general the

actors involved in the proceedings.

- Lawyers/Law firms shall undertake to refrain from using, invoking and in general processing personal data of persons who are not parties/actors involved in the proceedings, in particular in case of special categories of personal data of article 9 of the Regulation, personal data relating to criminal offences and convictions or data relating to minors, unless this is strictly necessary to establish, exercise or defend legal claims, and provided that the rights of the data subjects concerned are not overriding.

Regarding accuracy and keeping personal data up to date:

- Lawyers/Law firms shall ensure that the personal data processed are accurate and, where necessary, kept up to date.
- Lawyers/Law firms shall provide that personal data, in particular special categories of personal data or personal data relating to criminal offences or convictions, whose accuracy, completeness and updating has not been established, are not processed, except for storage purposes. Such data shall not, in particular, be disclosed or made available, transmitted and/or communicated to third parties, until their accuracy has been established or the necessary rectification and/or updating has been carried out.
- Lawyers/Law firms shall adopt appropriate measures and procedures to examine inaccurate personal data and to rectify, erase or keep them up to date. In case of personal data relating to or provided by their clients, the latter are required to verify the fact that the data are accurate and up to date. This declaration fulfils in principle the relevant obligation.
- Lawyers/Law firms, shall conduct without undue delay all necessary actions to immediately erase, rectify or update inaccurate personal data, having regard to the purposes for which they are processed, as soon as they establish or become aware of the

inaccuracy or the need for update.

Regarding storage limitation:

- Lawyers/Law firms shall keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed, otherwise for no longer than the period provided explicitly by law. Following that period, lawyers/law firms shall safely erase personal data and destroy the respective documents or return them to the data subjects.
- Lawyers/Law firms shall further retain personal data if this is necessary for compliance with a legal obligation, such as compliance with obligations under tax law.
- Lawyers/Law firms shall retain personal data beyond the time necessary for the purpose for which they are processed initially in order to establish, exercise and defend legal claims. In any case, the retention period shall not exceed twenty (20) years from the point in time when lawyers/law firms should have erased the data due to the fulfilment of the purpose for which the personal data were processed initially, except in the cases provided in paragraph 5.
- Lawyers/Law firms shall retain personal data for a longer period of time if the data subject consents, provided that she/he has been informed thereof.
- Lawyers/Law firms shall retain personal data for a period of time exceeding the aforementioned periods, provided that the data are processed for statistical or research purposes, and that they are anonymized or that appropriate and adequate organizational and technical measures for their safe retention are taken.

5. Legal bases for processing

For the processing of personal data to be lawful at least one of the

following conditions must be met:

A. The data subject has consented. As far as consent is concerned, the following applies:

- Consent is given freely, by a statement or a clear affirmative act of the data subject, which must be informed with regard to the conditions and purposes of the processing, specific and unambiguous. Explicit consent is required for the processing of special categories of personal data or personal data relating to criminal offences and convictions. Consent may be given by electronic means or by oral statement. Demonstrating consent, especially when provided orally, entails difficulties.
- Consent is withdrawn freely. It must be ensured that it is as easy to withdraw as to give consent. Prior to giving consent, the data subject is informed thereof. The subject is also informed that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Moreover, in case of withdrawal, the data subject is informed whether her/his data have been further processed or whether the processing will continue based on a different legal basis, such as compliance with a legal obligation or establishment, exercise or defence of rights.

Recommendations

- Develop standardized consent forms fulfilling all the legal requirements to be provided to the data subjects for all the cases relating to the activity concerned, where consent may be used as the basis of processing.
- Ensure identification of the person giving consent and authenticity/integrity of the electronic document/declaration, in cooperation with the competent technician, in case that consent is given by electronic means.
- In view of the accountability principle, create and maintain a record of consent statements by the Data Protection Officer (hereinafter referred to as the "DPO") or the person entrusted with monitoring compliance with the Code, including clear and unambiguous information on the identity of the person, prior information, the manner and time of giving consent.

B. The processing is necessary for the performance of a contract to which the data subject is party.

For example: The processing is necessary for the performance of a mandate contract concluded with the lawyer or the law firm, including the necessary processing operations. The contract shall include the conditions under which personal data are processed as well as the required information to the data subject, in accordance with the GDPR (including information on the purpose, the legal basis for processing, the categories of personal data, the recipients, the planned or estimated duration of data retention, the rights of the persons, and information regarding legal remedies and appeal).

C. The processing is necessary for compliance with a legal obligation to which the controller is subject.

For example: The processing is necessary for the compliance of lawyers and law firms falling under the provisions of the Code with the law - in particular tax law, law on professional practice and law on the fight against money laundering.

D. The processing is necessary in order to protect the vital interests of the data subject and the latter is incapable of giving consent.

A vital interest is considered as an interest which is essential for the data subject's or another person's life. Processing of personal data based on the vital interest of another natural person should in principle be carried out only where the processing cannot be manifestly based on another legal basis.

E. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.

F. The processing is necessary for the purposes of compelling legitimate interests pursued by the controller or a third party, which are not overridden by the legitimate interests of the data subject.

The establishment, exercise and defence of a right before a court, arbitration body, disciplinary body or mediation mechanism may be considered as a legitimate interest.

ATTENTION: The aforementioned conditions do not apply in the case of special categories of personal data, the processing of which in principle is prohibited, except under specific - stricter - conditions.

Recommendation:

The DPO, when designated (see below), or the person entrusted with the task of monitoring compliance with this Code performs a standardization of processing operations of special categories of personal data, typical in the context of the activity concerned, and establishes relevant procedures.

6. Rights of the Data Subject

Data subjects have the following rights:

- **Right of access and information:** The data subject has the right to know whether her/his data are being processed, as well as the means and purposes of the processing.
- **Right to rectification - updating:** The data subject has the right to obtain the rectification of inaccurate/incomplete personal data.
- **Right to erasure (right to be forgotten):** The data subject has the right to obtain the erasure of personal data, if they are no longer necessary and processing is not legally grounded.
- **Right to restriction of processing.**
- **Right to object processing.**
- **Right to data portability.**
- **Right to object automated individual decision-making**, including profiling.

6.1. Right to information

A. Where personal data are collected from the data subject, the controller shall, *at the time when personal data are obtained*, provide the subject with the following information at least:

- the identity and the contact details of the controller;
- the purpose or purposes of the processing;

- the legal basis for the processing;
- the categories of personal data that are going to be processed;
- the recipients / categories of recipients of the personal data;
- where applicable, the fact that the controller intends to transfer personal data to a third country and the legal conditions under which the transfer may take place;
- the period for which the personal data will be stored;
- the aforementioned rights of the subject;
- the right to lodge a complaint before the HDPA;
- the right to legal remedies and appeal;
- whether the provision of personal data is mandatory;
- the existence of automated decision-making, including profiling.

B. In case of processing of personal data for purposes different than the purpose for which they were originally provided, the data subject shall be informed beforehand.

C. Information shall be provided in a clear, comprehensible and concise manner, taking account of the specific characteristics of the data subject and the context of the processing.

D. Upon request of the data subject and after confirming her/his identity, the controller shall provide information without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Special attention shall be paid to provide the information requested only to the data subject or to an authorized person. As such, it is necessary to establish the person's identity by appropriate and safe

means. Failure to satisfy a request for information, in whole or in part, is permitted only if the data subject already has the information mentioned above or in so far as the restriction of access is required for/related to the establishment, exercise, defence or enforcement of legal claims and the exercise of the right to information would seriously impair or render impossible the achievement of the objectives of that processing.

Where requests are manifestly unfounded or excessive, they may not be satisfied or a reasonable fee may be charged.

6.2. Regarding the right to erasure

Controllers shall not have the obligation to erase personal data in cases where processing is necessary:

- For compliance with a legal obligation which requires processing by Union or member state law, such as for compliance with tax law;
- For scientific or historical research purposes or statistical purposes in so far as the erasure of personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing and provided that the technical and organizational measures provided by law for the protection of personal data, such as pseudonymization and anonymization, are taken;
- For the establishment, exercise or defence of legal claims of the controller or for the rebuttal of existing or potential legal claims of the data subject or a third part.
- Where the controller has transmitted or made public personal data and is obliged to erase them, the controller, taking account of available technology and the cost of implementation, shall inform controllers and processors that are processing the personal data that the data subject has requested the erasure,

so that they, in turn, erase any links to, or copy or replication of, those personal data, without prejudice to a different legal basis for their retention.

- Particular attention shall be paid to adhere to the right to erasure, especially in case of minors wishing to erase/exercising the right to erasure of their personal data.

6.3. Regarding the right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing of the personal data in the cases mentioned below. Such personal data shall only be processed with the data subject's specific and unambiguous consent for exceptional use, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of important public interest. Namely, the data subject shall request restriction of processing where one of the following applies:

- Where the accuracy of the personal data is contested by the data subject. In this case, the controller shall restrict processing for a period enabling the verification of the data's accuracy.
- Where the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- Where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- Where the data subject has objected to processing pursuant to article 21 of the Regulation, pending the verification whether the legitimate grounds of the controller override those of the data subject, for a period enabling such verification.

Recommendations

- Establish pre-determined procedures for the restriction of processing - such as measures for the restriction and control of access to personal data, or retention of personal data by a distinct body/in a distinct processing and/or storage record - and take any other appropriate measure. Always ensure and make clear to anyone with access to the personal data that their processing is under restriction.
- Delegate to a specific person the tasks of notifying the restriction to the recipients of the personal data and of communicating the lifting of restriction to the data subject, prior to the lifting, and determine the means of communication. It is recommended that the aforementioned tasks are allocated to the DPO, where applicable, or the person entrusted with monitoring compliance with this Code.

6.4. Regarding the right to data prortability

The data subject shall have the right to receive the personal data concerning her or him, which she or he has provided to a controller, and the right to request the latter to transmit those data to another controller without hindrance, where the processing is based on the data subject's consent or it concerns the performance of a contract between the data subject and the controller and it is carried out by automated means.

The controller shall either provide the personal data to the data subject or transmit them to another controller in a structured, commonly used and machine-readable format, where technically feasible.

The relevant request shall not be satisfied where the processing of the personal data is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. In any case, the right to receive the personal data should

be without prejudice to the rights and freedoms of other persons.

Recommendation

The right to data portability is not fulfilled in the following cases:

(List cases relating to the activity concerned, where non-adherence to the obligation pursuant to the right to data portability is justified).

6.5. Regarding the right to object processing

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning her or him which is based on point (e) or (f) of article 6(1) of the Regulation.

The controller shall respect the right and no longer process the personal data, unless the controller demonstrates compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning her or him for such marketing, which includes profiling to the extent that it is related to such direct marketing.

7. Obligations of Controllers and Processors

Controllers and processors are generally obliged to comply with all the provisions of the applicable legal framework and have increased accountability, as mentioned above.

Their basic obligations include inter alia:

7.1. Implementation of appropriate technical and organizational measures to ensure that processing is conducted in compliance with the Regulation

Security encompasses confidentiality, on the one hand, and availability and integrity, on the other.

An indicative list of security measures, such as pseudonymization and encryption, is included in article 32 of the Regulation. The measures to be taken always depend on the particular case.

Security measures shall be appropriate and proportionate to the risk. The relevant assessment shall take into account the state of the art with regard to technological developments, the number of employees, the workload, the number of partners and clients, the costs of implementation, the nature and category of the personal data that are processed and the context and specific purposes of processing.

In assessing the risk, account shall be taken in particular of its likelihood and severity, especially with regard to the protection of personal data and the rights and freedoms of data subjects in general.

Recommendations

List necessary security measures and procedures relating to the activity concerned.

Examples:

- Set out technical and organizational measures for data security and protection, especially from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Subject partners to relevant contractual clauses.
- Establish mechanisms of classification and control of access to processing and files (filing systems) that contain personal data.

- Determine measures for secure destruction of data and material carriers of data (see HDPA Guidance 1/2005).
- Ensure systematic protection against malicious software, viruses, attacks on information systems, data corruption etc. and controls on a regular basis.
- Adopt policy of physical security and policy of "clean office" ("locking files", locking computers, protected printing etc.)
- Perform encrypted back-up on a regular basis.
- Adopt policy of limited use of portable and removable devices and establish technical measures and procedures for their appropriate use.

7.2. Data protection by design and by default

This obligation means, first and foremost, that the appropriate technical and organizational measures and relevant safeguards must be enacted by data processors at the initial stages of each application's design. In fact, these measures should correspond to the current state-of-the-art.

The obligation for data protection by default means that from the moment the decision on data processing is made, the impending processing must be limited to the data which is absolutely necessary to achieve the specific purpose of processing.

The fulfilment of this obligation may incur some costs. These costs should be forecast in the project's budget. Finally, the principle of accountability applies in this case as well. Therefore, data subjects should have information available on how this obligation is being fulfilled.

7.3. Maintaining a record of processing activities

I.e. maintain a record by means of documenting all processing activities, in accordance with article 30 of the Regulation. This obligation applies in cases where:

- the processing that is being carried out is likely to result in a risk to the rights and freedoms of data subjects;
- the processing is not occasional; or
- the processing includes special categories of data or data concerning criminal convictions and offences.

Recommendation

Maintain and update a record of processing activities on a regular basis, even in cases that the Regulation does not impose such an obligation. Maintaining such a record is crucial in terms of accountability and, in addition, it serves as a useful means of compliance.

The record of processing activities shall contain, as a minimum:

(a) the name and contact details of the controller;

(b) the purposes of the processing;

(c) a description of the categories of data subjects;

(d) a description of the categories of personal data (with special reference to special categories of data and data concerning criminal convictions and offences);

(e) the categories of (typical) recipients to whom the personal data have been/are usually being/ are required to be disclosed;

(f) transfers of personal data to a third country (outside the EU/EEA);

(g) the envisaged time limits for erasure; and

(h) where possible, a general description of the technical and organizational security measures.

The form of the record of processing activities is not specified (see relevant form on the website of the Cypriot and Greek DPAs).

7.4. Assessment of the impact of the processing

An assessment of the impact of the processing is required where it is likely to result in a high risk to the rights and freedoms of persons, in particular where it is carried out on a systematic basis or on a large scale, it concerns special categories of data, or it is based on the use of new technologies. Where processing involves a high risk, the controller should consult the national DPA prior to the processing.

The assessment shall contain at least:

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

(b) reference to the legal basis/ground for the processing, especially in cases where it is based on an overriding legitimate interest;

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

(d) an assessment of the risks to the rights and freedoms of data subjects; and

(e) the measures envisaged to address the risks, including safeguards, security measures and mechanisms.

Recommendation

Carry out an impact assessment in the following typical cases:

List specific cases where impact assessment is required or deemed appropriate for the activity concerned.

7.5. Conclusion of contracts with processors

According to the Regulation, a series of contractual clauses should be included in the contracts concluded between controllers and processors.

Recommendation

List the most typical cases, relating to the activity concerned, where controllers use processors, and establish pre-determined standard contractual clauses in full compliance with the Regulation.

7.6. Facilitation of the exercise of the rights of data subjects

Recommendation

Draft documents to facilitate the exercise of the data subjects' rights (see Annexes).

7.7. Designation of Data Protection Officer (DPO)

The function of the DPO guarantees accountability. In addition, it confers an advantage in terms of compliance with the legal framework for personal data protection.

The DPO is a natural or legal person that is designated by the controller (as well as the processor) and undertakes the tasks and responsibilities foreseen by the Regulation in order to support compliance with its requirements.

7.7.1. Mandatory designation of a DPO

The designation of a DPO is required in cases where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of

processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The notion of "large scale" processing was further defined and determined by the Article 29 Data Protection Working Party (hereinafter referred to as the "WP29"). Even though it is not possible to give a precise number with regard to the amount of data processed in order to define large scale processing, the following factors shall be taken into consideration:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population;
- The volume of data and/or the range of different data items being processed;
- The duration, or permanence, of the data processing activity; and
- The geographical extent of the processing activity.

Examples of large-scale processing include processing of patient data by a hospital, processing of customer data by an insurance company or a bank etc. Processing of patient data by an individual lawyer or doctor do not constitute large scale processing.

As far as the notion of regular and systematic monitoring is concerned, the WP29 recommends that the following elements should be considered.

The monitoring may be considered as regular where it is:

- ongoing or occurring at particular intervals for a particular period;
- repeated at fixed times; and
- constantly or periodically taking place.

The monitoring may be considered as systematic where it is occurring according to a system and it is:

- pre-arranged, organized or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

Examples of activities that may constitute a regular and systematic monitoring of data subjects include providing telecommunications services and data-driven marketing activities.

In case of doubt as to whether the designation of a DPO is mandatory, the WP29 encourages designation on a voluntary basis.

Recommendation

(On a case-by-case basis) Determine whether the designation of a DPO on a voluntary basis is recommended or is not recommended for the activity concerned.

ATTENTION: In case of designation on a voluntary basis, the DPO shall undertake all the tasks and duties as if the designation had been mandatory.

ATTENTION: The obligation to designate a DPO is neither static nor is it examined once and for all: undertaking new activities, carrying out new processing operations relating to the same activity, using new data, extending the scale of processing and other factors may render the designation of a DPO mandatory.

In case the DPO had initially been designated on a voluntary basis, it shall be documented and mentioned that the initial designation on a voluntary basis has subsequently been rendered mandatory.

7.7.2. Capacity and designation process

The DPO may be an internal employee, an external partner or an internal employee supported by an external partner. The choice

depends on a series of factors, such as the nature of the processing activities, the size of the organization, the need for support by a DPO and financial factors.

The function of the DPO can be exercised on a service contract basis (concluded with a natural or legal person). In case of a partner or a staff member, special attention shall be paid to avoid conflict between the tasks relating to her/his designation as a DPO and other tasks already assigned to her/him.

The DPO is designated in writing, by contract or an internal decision, defining the position, the tasks and the manner of performing the relevant function. The designation shall be made for a specific period of time and can be renewed. The designation may be revoked and the DPO may be dismissed only on grounds of major importance and under no circumstances for performing her/his tasks.

The DPO does not receive any instructions regarding the exercise of his or her tasks. The DPO should not be dismissed or penalized for performing her/his tasks (promptly and consistently).

The designation is communicated to the national DPA and to the public via public announcement, which includes the DPO's contact details.

The following persons shall not be designated as DPOs:

- management staff, such as the managing director and the financial director (list cases);
- human resources, information technology and marketing managers;
- other staff that may determine new purposes and means of processing.

A group of undertakings may designate a single DPO provided that she or he is easily accessible from each establishment.

7.7.3. Selection criteria

The DPO's selection criteria are not set out in detail in the Regulation. As per article 37 para. 5 "The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in article 39".

According to the WP29, the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

In any case, the DPO should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. She/he should also have an understanding of the processing operations carried out, knowledge of information systems, data security, the business sector and the organization, and the ability to foster a data protection culture within the organization. In addition, easy and regular access to all establishments of the organization, where processing of personal data takes place, should be ensured for the DPO - both in terms of feasibility and in terms of fulfiling her/his duties.

At the same time, accessibility means that the DPO her/himself should be easily accessible by the data subjects and the supervisory authority.

Technically, the DPO is not required to be a lawyer. However, it should be taken into consideration that the Regulation is a legal document, drafted by lawyers. As such, a lawyer might find it easier to deal with questions of interpretation and implementation. Nevertheless, even though an in-depth understanding of the Regulation is required, it cannot be considered as a sufficient selection criterion per se, especially in cases where the organization processes special types of data that the

DPO is not acquainted with.

Fpr example: a lawyer with several years of previous experience on data protection law is negotiating the position of DPO with a big digital marketing company. However, the lawyer does not have experience on issues relating to computers and the internet. In case the lawyer is designated as a DPO, she/he should be acquainted with issues relating to digital marketing and the specific processing operations of the market and the management should support her/him.

Since 2010, the European Union has set out best practices for the selection of DPOs of its institutions and bodies; Regulation (EU) 45/2001 on the processing of personal data by the Community institutions and bodies has already been applicable for a long time. Relevant requirements should be applied for the DPOs of public authorities and bodies, as well as of commercial enterprises.

Recommendations

The DPO shall fulfil the following conditions, namely she/he shall:

- Understand in-depth the Regulation, national legislation on personal data, decisions issued by supervisory authorities, information systems and data security.
- Have a good understanding of the function and the processing operations of the organization in question and be aware of the specific regulatory framework governing the organization.
- Have the possibility to conduct regular on-site visits to the premises where processing is carried out.
- Be continuously accessible (in terms of language of communication as well) by the data subjects and continuously communicate with the national DPA.

ATTENTION: No certification procedure for DPOs is provided. The

requirement of certification as a necessary qualification for the designation of a DPO of a public authority has been declared unlawful in an EU member state.

7.7.4. Tasks and duties

Article 39 of the Regulation sets out the tasks of the DPO, namely:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Regulation and to other Union or member state data protection provisions;
- to monitor compliance with the Regulation, with other Union or member state data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 35;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in article 36, and to consult, where appropriate, with regard to any other matter.

Additional tasks relating to the obligations deriving from the Regulation may be assigned to the DPO and it would be appropriate for her/him to undertake them. These tasks may include maintaining the record of processing operations and planning internal policy concerning its updating in case of new processing activities, coordinating activities for the formation of data security policies, business continuity policies,

confidentiality policies and a special plan of managing incidents of data leakage or breach and keeping a register of requests received by data subjects.

The role of the DPO is advisory and not decisive: it is for the organization's management to decide upon the actions proposed by the DPO.

The DPO has access to all the records, electronic and written, and all the systems relating to the processing of personal data.

7.7.5. Position of the DPO within the organisation

Article 38 of the Regulation imposes a series of obligations with regard to the DPO's position and independence. Namely, organizations shall:

- Ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data;
- Support the DPO in performing the tasks referred to in article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and resources necessary to maintain his or her expert knowledge; and
- Ensure that the DPO does not receive any instructions regarding the exercise of those tasks and that she/he shall not be dismissed or penalized by the controller or the processor for performing her/his tasks.
- Provide that the DPO shall directly report to the highest management level of the organization that shall respond to the requests.
- Create appropriate mechanisms and communication channels between data subjects the DPO; the DPO is obligated to respond to them.

Last but not least, the fact that "The data protection officer shall be

bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or member state law", according to article 38 para. 5, is particularly important. The DPO should keep any data and information obtained during the performance of her/his tasks confidential. This duty may also extend to the organization's management. The DPO should not communicate or disclose events or information that have come to her/his knowledge in the course of the performance of her/his tasks to a third party. She/he should generally respect confidentiality concerning the performance of her/his tasks, in accordance with the applicable legal framework. The DPO is subject to the aforementioned duties both during and after the termination of her/his designation. More specific duties concerning confidentiality may be imposed by the designation act.

7.7.6. Actions to be undertaken by the DPO – Basic Guide

A. Distinguishing the processing activities for which the organization acts as a controller, as opposed to the activities for which it acts as a processor, is the first issue to be addressed by the newly designated DPO. The distinction is important for a series of reasons, mainly in order for the organization to fulfil its obligations to its counterparties, in compliance with article 28 of the Regulation.

B. The DPO's responsibilities are determined to a large extent by the nature of the processing activities.

C. Moreover, it is recommended that the DPO is informed in advance about the categories of data that the organization processes, such as financial data, medical data, data concerning the organization's staff or consumers as well.

D. Any additional responsibilities of the DPO should be agreed in advance, according to article 38 para. 6 of the Regulation, which provides that "The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and

duties do not result in a conflict of interests". Such "other tasks" may not result in a conflict of interest but may nevertheless prevent the DPO from performing her/his duties within the organization.

E. Upon deciding to assume the position of DPO, she/he should be rapidly informed about the current situation and acquaint her/himself with the facilities, the staff and the organization in general.

F. The ideal mentor for the new DPO is the previous one, if any. Regardless of the reasons for which she/he no longer performs her/his function, the old DPO is essentially the only one who is aware of the level of compliance of the organization, the shortcomings and the outstanding issues. The new DPO should attempt to contact her/his predecessor concerning issues of internal cooperation and communication within the organization as well: who can help her/him, whether the DPO is considered as unnecessary burden or obstacle for business or whether she/he can expect good cooperation with the organization's departments and units.

G. The new DPO should consider prior actions with regard to compliance, namely examine the work already performed and ensure that is completed, updated and/or revised.

H. The DPO should establish whether the organization's confidentiality and security policies are observed, as well as the level of implementation of the necessary actions – in terms of both electronic (for example, cyber security) and physical security (for example, accessibility of premises to visitors, entry checks in workplaces, video recording and equipment).

I. The DPO should determine whether there are pending issues with the Authority and data subjects. Once the designation of the new DPO is communicated to the Authority, she/he shall be confronted with all the relevant issues. Upon undertaking her/his tasks, among other issues, the DPO may have to deal with a series of problems including cases

already pending before the Authority and requests by the subjects concerning the exercise of their rights. Data subjects' requests in exercise of their rights deriving from the Regulation shall be satisfied within the time limits generally provided by the Regulation (in principle, within thirty days). The DPO should examine existing requests, prioritize actions with regard to their handling depending on their difficulty and communicate with other departments of the organization to provide services, if necessary. It should be taken into consideration that new requests will be added to the existing ones. In addition, the level of difficulty in terms of the fulfilment of the data subjects' rights should serve as a basic criterion for prioritization by the DPO.

J. The DPO should conduct meetings with department heads and proceed to internal consultations. Once the aforementioned actions have been completed, it is recommended that the DPO conducts internal meetings with the heads of the various departments that perform data processing. In cases of organizations providing services to individuals – such as insurance companies, hospitals etc. – the DPO's first concern should be to communicate with the managers of the commercial department, the sales department, the customer service department and so forth in order to address the issues initially identified. If, on the other hand, the organization does not deal with natural persons, priority should be given to human resources issues.

7.7.7. Fostering a data protection culture

The DPO's duties are of a dual nature: on the one hand, she/he provides guidance with regard to the organization's activities that are related to data processing, in compliance with the Regulation and the relevant legal framework, and, on the other hand, she/he fosters a data protection culture within the organization.

The DPO shall disseminate among the staff an attitude of adhering to data protection, not only for the sake of the organization's overall

interest but also in a broader sense. She/he shall highlight the reasons why each staff member should be vigilant against the risk of loss and alteration of the data she/he is processing individually, fostering an attitude of individual responsibility.

The aforementioned task may be accomplished through regular training events: the DPO can organize seminars and train the staff, especially in case of small organizations with few staff members. In case of larger organizations, the DPO can train or ensure the training of selected higher-ranking staff - for example, the Human Resources Directorate - who will in turn undertake the training of lower-ranking and newly deployed staff.

Newly recruited staff shall be trained first, as they are sensitized more easily and, thus, adopt relevant policies immediately. Training shall continue on an annual basis, until the entire organization has been covered. Groups shall be separated on the basis of common interest and scope of activity (dealing with customers or co-workers).

7.7.8. Continuous education and training of the DPO

Continuous education and training of the DPO and the staff that support her/him is a prerequisite for the proper performance of her/his duties. The law on the protection of personal data is dynamic and constantly evolving: first of all, the DPO her/himself should demonstrate initiative with regard to her/his continuous education and training. The organization should provide material support to that end, by providing resources to the DPO to maintain her/his expert knowledge (article 38 para. 2 of the GDPR).

In addition, the DPO is recommended to pursue training on issues related to her/his organization's sector. In case of institutional changes - such as in labor law - the DPO is required to stay up to date, individually or together with the organization's legal advisers, in order to be able to examine the implications on relevant data processing.

7.7.9. In summary

- The DPO performs her/his tasks in an independent manner, taking account of the protection of personal data, even if her/his opinion is at odds with the organization's position.
- The DPO advises on data protection issues in the most appropriate manner. The advice should be provided in an objective, substantiated and transparent manner.
- Professional diligence demonstrated by a prudent professional requires that she/he does not undertake the position of DPO, if she/he does not consider that she/he fulfils the necessary requirements.
- The DPO pursues education and continuous training on personal data law and information security, staying up to date with regard to technological and other developments in the sector.
- The DPO is actively involved in every matter concerning personal data.
- Fostering a data protection culture within the organization by all appropriate means is a basic concern of the DPO.
- The DPO requests the necessary resources, such as time, infrastructure, funds and supporting staff in order to fulfil her/his tasks.
- The competent director or the management should inform the DPO about all processing operations carried out by the organization.
- The DPO provides advice on data protection by default and by design before the organization introduces changes in data processing and undertakes new processing activities.
- The DPO is easily accessible to data subjects, both inside and outside of the organization, and her/his contact details are publicly available.

- The DPO informs the management of the organization on a regular basis. In this case, it is recommended that the DPO drafts activity reports periodically (for example, on an annual basis), within a specific timeframe (for example, each January, covering the period of the previous year).
- The DPO ensures that internal audits are conducted on a regular basis in order to safeguard the organization' s compliance with the basic principles and obligations pursuant to the Regulation. In this case, regular audits must be conducted periodically (for example, every six months).
- At the beginning of each year, the DPO prepares an action plan for the following year, taking into consideration the organization's needs, and she/he submits requests for additional resources.
- When dealing with data subjects' requests and complaints, the DPO shall decide on their grounds and legality in an objective manner and respond in a timely and professional manner.
- The DPO shall avoid to undertake any task or duty that may result in a conflict of interests and shall refrain from any other undertaking that may impact negatively on her/his tasks.
- All the information managed by the DPO shall be kept confidential.

7.7.10. Obligation to notify personal data breach

In the case of a personal data breach, within the meaning of article 33 of the Regulation, the controller shall without undue delay and, where feasible, **not later than 72 hours after having become aware of it**, notify the breach to the national DPA. Even if all the relevant information is not available at the time of notification, an initial notification should be submitted, without undue delay, and more information should be provided in phases without undue further delay.

Notification is not required if the personal data breach is unlikely to

result in a risk to the rights and freedoms of data subjects.

When assessing the risk and severity of the breach, a series of factors shall be taken into consideration, including:

(a) the nature, volume and category of personal data affected by the breach;

(b) the possibility to identify the data subjects;

(c) the severity of the consequences of the personal data breach for the data subjects;

(d) the status, number and special features of the data subjects (for example, defendants, witnesses, minors etc.).

There is a presumption of serious risk where the personal data breach may result in physical, material or non-material damage of a natural person, such as: risk of making personal data public, risk to life or physical integrity of data subjects, identity theft, damage to reputation or infringement of personality rights, serious material damage or damage to legitimate interests, loss of confidentiality in case of personal data subject to professional or other secrecy according to the law.

In case of attempted breach, the rights and freedoms of data subjects are not endangered; therefore, no notification to the national DPA is required.

The national DPA has produced standard forms, which can be used to submit a personal data breach notification (see Annexes).

ATTENTION: An internal record of incidents of breach that took place but were not notified to the national DPA, because it was considered that they could not result in a risk to rights and freedoms of the data subjects, must be kept. The record shall include a brief description of each incident, as well as of the reasons for which it was considered that it does not give rise to a notification obligation.

Where the personal data breach is likely to result in a high risk to the

rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication to the data subject is not required if any of the conditions foreseen in article 34 para. 3 of the Regulation are met, namely where the controller has implemented appropriate technical and organizational protection measures (such as encryption, restriction of access to physical file etc.) and those measures were applied to the personal data affected by the breach, rendering the personal data unintelligible to any person who is not authorized to access it; where the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; and where the notification is impossible or it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

8. Specific issues

Issues relating to the activity regulated by the Code shall be examined, for example:

- Processing of personal data of trainee lawyers.
- Cross border flows in the course of legal practice.
- Video surveillance systems [if such systems are commonly used, the applicable legal framework – Regulation and domestic law provisions, impact assessment, decisions and recommendations by the Authority and the competent European bodies – and best practice recommendations shall be mentioned] etc.

9. Sanctions

Civil law claims may be raised by data subjects who have suffered damage on account of a personal data breach. In addition, administrative sanctions (fines) of up to 20,000,000 EUR or 4 % of the total worldwide annual turnover – graduated according to the nature of the

infringement – are foreseen by the Regulation.

Criminal sanctions are foreseen by the national law.

CHECK LIST

15 steps towards compliance

- ✓ 1. Document all data processing activities that are being carried out. Pay special attention to processing of special categories of personal data, which are addressed separately.
- ✓ 2. Document the purpose of every processing operation in an honest and accurate manner.
- ✓ 3. Indicate the legal basis of every processing operation. Limit processing on the grounds of consent to a strict minimum.
- ✓ 4. Ensure processing of adequate, up to date and accurate data, which is limited to what is necessary in any case. Establish relevant procedures of periodic review.
- ✓ 5. Register every person with access to personal data, for every processing operation. Verify the respective legal grounds.
- ✓ 6. Determine the period for which the personal data are retained. Include separate provisions for the period of data retention for typical, very common cases, such as personal data of candidates for recruitment, former employees, suppliers, partners and clients.
- ✓ 7. Ensure security of the establishments in general and security of the systems in particular. Designate a security officer. Verify the storage conditions of digital and non-digital files. Establish control procedures and regular review.
- ✓ 8. Determine procedures of safe destruction of personal data, upon completion of the period of their retention. Assign this task to specific persons.
- ✓ 9. Examine every transfer of personal data to third countries and its legal grounds.
- ✓ 10. Pay special attention to the requirements for legitimate

operation of video surveillance systems.

- ✓ 11. Establish general procedures for the selection of adequate technical and organizational measures.
- ✓ 12. Review staff contracts, as well as contracts with partners and suppliers.
- ✓ 13. Establish procedures to fulfil rights and to notify breaches.
- ✓ 14. Organize regular staff trainings and other awareness-raising activities relating to personal data protection.
- ✓ 15. Establish regular monitoring of the record foreseen in article 30 of the Regulation.

PART C

After the implementation of the Code

C1. Monitoring compliance with the Code

Monitoring compliance with the provisions of the Code shall be entrusted to a single person or a group of persons, whose tasks shall be divided per subject-matter.

If a single person is chosen, the task shall be assigned to the DPO, where applicable.

C2. Regular review – updating of the Code

The Code shall be reviewed and updated every two years and, in any case, whenever the legal framework changes. The person mentioned above (under C1) shall be entrusted with this task.

Recommendations

- Consult with the persons to whom the Code applies before each review.
- Organize a presentation event (workshop/seminar) following each review.
- Send a draft of the reviewed Code to the national DPA for comments and observations before finalizing it.

C3. Introduction of sanctions for failure to comply with the Code

Persons infringing the provisions of the Code shall be liable to some form of consequences.

It remains at the discretion of whoever adheres to the Code to determine the nature of those consequences. However, it is recommended that the obligation of compliance with the Code should be associated to the general regulatory framework governing the

employees' obligations, on the one hand, and to the evaluation system, on the other.

Part D

Annexes

1. Documents for the facilitation of data subjects in the exercise of their rights.
2. Forms for response to breach incidents.
3. Legal Documents.
4. Regulation (EU) 2016/679.
5. 3.2. Law 4624/2019.
6. Legal framework applicable to the activity concerned (for example, Code of Lawyers).
7. On the need for an impact assessment study: Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, 5 April 2017.
8. On DPOs: Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, 5 April 2017.
9. 3.6. Caselaw of the national DPA and the courts relating to the activity concerned.

CENTRE FOR EUROPEAN CONSTITUTIONAL LAW
THEMISTOKLES AND DIMITRIS TSATSOS FOUNDATION

University of Cyprus

HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837