Sample Good Practice Material Report

Deliverable D2.2

Editors
Efrosini Siougle (HDPA)
Kalliopi Karveli (HDPA)
Contributors
Maria Alikakou (HDPA)
Charikleia Latsiou (HDPA)
Elena Maragou (HDPA)
Stefania Plota (HDPA)
Leonidas Roussos (HDPA)
Charis Symeonidou (HDPA)

Reviewers
George Lioudakis (ABOVO)
Vasilis Zorkadis (HDPA)

Date
25th October 2021

Classification
Public

The byDesign project has received funding from the European Union's
Rights, Equality and Citizenship Programme (REC) under grant agreement No. 101005833

Table of Contents

1 Introduction

The byDesign project aims to provide assistance to SMEs and other relevant stakeholders, through developing appropriate compliance kits and training programmes, with respect to addressing the challenges stemming from the effective implementation of the GDPR. In this context, one of the main pillars of the project is the development of a compliance kit for SMEs, facilitating self-assistance for SMEs with a set of context-aware templates of essential documents and online tools. To this end, after having identified the needs and current gaps regarding the GDPR compliance of SMEs in Task 2.1, a sample good practice material is assembled reflecting broadly identified good practices in the topics addressed by and assessed in the aforementioned Task 2.1.

1.1 Purpose of the document

This document aims to present all good practices related material and the compliance methodology to be offered through it for SMEs'. More precisely, this document presents the topics addressed by the sample good practice material, how the material and the content tiles were created and assembled and the methodological framework for the generation of suitable and adaptable sample guidance documents to the SMEs based on the contextual information on each particular data controller. Moreover, it presents and describes the specific topics addressed by the sample material templates, their purpose and benefits for the SME's and it concludes by assessing how the sample material will contribute to the compliance of the SME's with the GDPR.

1.2 Relations to other activities in the project

Task 2.2 uses as a basis the need analysis and the relevant findings of Task 2.1, whose main goal was to assess the main needs and to elucidate the requirements for SME's compliance with GDPR. More specifically, this task will start by defining the topics addressed by the online tool, will continue with assembling the material reflecting broadly identified good practices in these topics and will result in a contextual framework providing SMEs with suitable sample documents based on their characteristics, thus significantly facilitating their compliance process. Subsequently, the aim of Task 2.3 is to be able to present in a meaningful and user friendly way the different kinds of guidance material accumulated throughout Task 2.2.

1.3 Structure of the document

This document consists of four sections, including the current introductory section. More precisely, the structure of the document is as follows:

- Section 2 describes the methodology of the task-analysis. More specifically, it contains information about the topics addressed by the sample good practice material, how the material was assembled, how the content tiles were created and the methodologic framework for the generation of the sample good practice material.
- Section 3 presents and describes the sample good practice documents, their purpose and their benefits for the SME's.
- Section 4 explains how the guidance material will contribute to the compliance of the SME's with the GDPR.
- Finally, the Appendix contains the sample good practice documents.

2 Methodology of the task - analysis and description

2.1 Definition of the topics addressed by the online toolkit

Task 2.2 ("Sample good practice material") of the byDesign project has received useful input from the deliverable produced by the Task 2.1 ("Need Analysis"). The requirements identified through the stakeholders from Task 2.1 constitute the basis for the definition of the topics addressed by the online compliance toolkit i.e. the concrete types of guidance to be offered, e.g., data protection policies, data subjects' rights exercise templates, web site related policies, terms of use, model clauses for subcontractors, sample texts for satisfying the transparency of the data processing, model records of processing activities. Through this online toolkit the actual sample good practice material that corresponds to each of the topics addressed will be available to the SMEs.

The general functional requirements of the easily extensible online toolkit as specified in Task 2.1 indicate the existence of an online wizard which would require as input identity and contact data of the SME, the business sector to which it belongs (from the ones specified in the deliverable namely Commerce, Tourism and Hospitality, Education, Health and other sectors) and the typical activities of the SME. The toolkit will provide as output several adaptable document template, notices that can be integrated into websites, educational material, guidelines and simplified texts/FAQs.

The topics addressed by the online toolkit focus on the following major areas, each one elaborated in types of guidance to be offered:

A. Lawfulness and transparency
1. The Provision of Information from SMEs to Data Subjects
2. Consent
3. Data protection rights and data subject request handling procedures
4. Destruction of personal data

B. Accountability
1. Records of processing activities
2. Security measures
3. Data breach handling
4. Assignment of data processing to contractors/processors

C. Business activities entailing data processing
1. Website
2. Direct marketing through electronic means
3. Video surveillance
4. Employee records

2.2 Assembling the material

Task 2.2 continues with assembling the material reflecting broadly identified good practices in the above major topics with the relevant sub-categories. This work extends along two directions: i) creation of the content tiles, i.e., fundamental parts for each document comprising the major topics specified in section 2.1, that will be consequently used to populate the actual instances of the documents based on the specific characteristics of an SME data controller; ii) the methodological framework for the generation of concrete document instances based on the contextual information on the particular data controller, such as the sectors that the controller belongs,

the data types collected, the processing operations it performs, the underlying purpose, complementary legal obligations (e.g., sectorial laws requiring data retention), etc.

Based on these two directions, byDesign will result in a contextual framework providing SMEs with suitable sample documents based on their characteristics, thus significantly facilitating their compliance process.

2.2.1 Creation of the content tiles

In order to create the content tiles of the sample good practice material for providing guidance to the SMEs on the major areas presented in section 2.1 the following steps were followed:

1. Step 1: gathering of information and studies related to the characteristics of the main processing operations of the SMEs based on the typical activities they perform in each of the selected sectors (namely Commerce, Tourism and Hospitality, Education, Health and other sectors).
2. Step 2: identification of common categories of processing operations between the above sectors as well as specific processing operations relevant to each specific sector. The main data processing purposes related to each category of processing operations along with significant categories of personal data collected were also identified.
3. Step 3: following the analysis from the previous two steps, the third step was devoted to the specification of the sample good practice documents corresponding to each of the topics addressed by the online toolkit, as described in section 2.1. To be useful and comprehensive, the guidance material consisted of both templates and simplified information material in the form of Frequently Asked Questions, according to the specific requirements of each topic and covering the most important areas of interest. More specifically, for several topics, the templates were drafted corresponding to the selected business sectors of the SMEs while for other topics the templates were drafted to be applicable to all sectors.
4. Step 4: the content outlines of each guidance document was specified.
5. Step 5: the analysis from the previous steps was presented to the partners of the byDesign project and their comments were incorporated.
6. Step 6: the content tiles were drafted based on the outlines from step 4 i.e. the fundamental parts for each guidance document that will be used for the generation of concrete document instances based on the contextual information of the particular SME.
7. Step 7: the content tiles were presented to the partners of the byDesign Project and their comments were incorporated.

The main processing operations of the SMEs in the selected sectors are identified as follows:

1. Customer/client management

The processing operations of the SMEs related to customer/client management are dependent on the sector to which they belong and especially to the major business activity of the sector. The main business activity of each SME for the above four sectors may be further specified on the basis of the Business Activity Code.

- Health sector: provision of health care services, collection of health data (medical history, dates of visit, type of service provided, treatment, insurance capacity, details of any private insurance etc.).
- Education sector: provision of education services (private schools, language schools, Greek language courses) etc., collection of health data (pupil's health card information) as well as study and conduct details.

- Tourism – Hospitality sector: provision of hotel and tourist services (hotel, accommodation, catering) etc., collection of health data (e.g. any allergies, disabilities) and preferences (e.g. any dietary preferences).
- Commerce sector: supply of retail trade services of products including distance e-shop services, collection of transaction and history data, data about participation in customer loyalty/bonus programs.

The following processing operations are common between the selected sectors and any other sector specified by the SME or added in the future extension of the online toolkit.

2. **Personnel management**
3. **Management of prospective employees**
4. **Management of suppliers-natural persons**
5. **Video surveillance**
6. **Direct marketing to potential customers**
7. **Data breach management**

Following the above analysis, the description of the documents comprising the sample good practice material for each topic addressed in the online toolkit is presented in Table 1.

Table 1. Sample good practice guidance documents		
A. Transparency and lawfulness		
A1	**Transparency**	1. Frequently Asked Questions for the provision of information to data subjects – transparency
A2	**Templates for the provision of information from SMEs to data subjects (based on the relevant processing operation)**	1. Template for the provision of information to customers/clients – Health sector 2. Template for the provision of information to customers/clients – Education sector 3. Template for the provision of information to customers/clients – Tourism-Hospitality sector 4. Template for the provision of information to customers/clients – Commerce sector 5. Template for the provision of information to customers/clients – Other sector 6. Template for the provision of information to potential customers (for all sectors) 7. Template for the provision of information to suppliers-natural persons (for all sectors) 8. Template for the provision of information to employees (for all sectors) 9. Template for the provision of information to prospective/candidate employees (for all sectors) 10. Template for the provision of information to individuals in case of a personal data breach (for all sectors) 11. Template for the provision of information on video surveillance (for all sectors) 12. Template for the provision of first level (A-level) information on video surveillance (for all sectors) 13. Template for the provision of second level (B-level information) on video surveillance (for all sectors) 14. Table matching the data processing purposes for each processing operation with the relevant legal bases and data subjects' rights
A3	**Consent**	1. Frequently Asked Questions about consent as a legal basis for personal data processing 2. Template of a customer's declaration of consent for photography and video recording of a private school event 3. Template of an employee's declaration of consent on the collection of material from social events and/or promotional activities 4. Template of an employee's declaration of consent on optional benefit 5. Template of a prospective employee's declaration of consent

A4	**Data protection rights and data subject request handling procedures**	1. General information (in the form of FAQs) about the exercise of the data subjects' rights 2. Request form for the exercise of right of access (article 15 GDPR) 3. Specific information and how to exercise the right of access (in FAQ form) 4. Request form for the exercise of right to rectification (article 16 GDPR) 5. Specific information and how to exercise the right to rectification (in FAQ form) 6. Request form for the exercise of right to erasure (article 17 GDPR) 7. Specific information and how to exercise the right to erasure (in FAQ form) 8. Request form for the exercise of right to restriction (article 18 GDPR) 9. Specific information and how to exercise the right to restriction (in FAQ form) 10. Request form for the exercise of right to data portability (article 20 GDPR) 11. Specific information and how to exercise the right of portability (in FAQ form) 12. Request form for the exercise of right to object (article 21 GDPR) 13. Specific information and how to exercise the right to object (in FAQ form) 14. Request form for the exercise of the right not to be subject to automated individual decision-making/profiling (article 22 GDPR) 15. Specific information and how to exercise the right not to be subject to automated individual decision-making/profiling (in FAQ form)
A5	**Destruction of personal data**	1. Frequently Asked Questions about the destruction of a personal data file 2. Sample template of a File Destruction Policy 3. Sample template of a File Destruction Protocol
B. Accountability		
B1	**Records of processing activities**	1. Model records of processing activities for customer management in the Commerce sector 2. Model records of processing activities for customer management in the Tourism-Hospitality sector 3. Model records of processing activities for customer management in the Education sector 4. Model records of processing activities for customer management in the Health sector 5. Model records of processing activities for employee management (for all sectors) 6. Model records of processing activities for management of prospective employees (for all sectors)

		7. Model records of processing activities for management of suppliers-natural persons (for all sectors) 8. Model records of processing activities for video surveillance (for all sectors) 9. Model records of processing activities for direct marketing to potential customers (for all sectors) 10. Model records of processing activities for personal data breach management (for all sectors) 11. Frequently Asked Questions for the records of processing activities
B2	**Security measures**	1. List of basic organizational and technical security measures for the SMEs
B3	**Data Breach handling**	1. Information and procedures for the SME on how to identify and handle personal data breaches a) internally in the SME, b) towards the data subjects affected, and c) towards the Data Protection Authority 2. Employee awareness leaflet on personal data breaches
B4	**Assignment of data processing to contractors/processors**	1. Frequently Asked Questions for processors 2. General template Appendix regarding data processing to a signed contract between the SME, as controller, and the company acting as processor 3. Specific template Appendix to a signed contract for processors that provide services of promoting products and services (marketing) 4. Specific template Appendix to a signed contract for processors that are cloud service providers
C. Business activities entailing data processing		
C1	**Website requirements in terms of transparency, basic security measures and compliance with cookies**	1. Checklist of clear requirements for a business website regarding transparency 2. Checklist of clear requirements for a business website regarding the security measures 3. Checklist of clear requirements for a business website regarding compliance with cookies
C2	**Direct marketing through electronic means**	1. Frequently Asked Questions for electronic direct marketing 2. Instructions for sending e-newsletters combined with a model information text and template e-mails
C3	**Video surveillance**	1. Frequently Asked Questions on video surveillance systems 2. Checklist of clear requirements for installing and operating a video surveillance system

C4	**Management of employees records and prospective employees records**	1. Frequently Asked Questions on the processing of employees' data 2. Frequently Asked Questions for processing of prospective employees' data 3. A template of a Use of Electronic Media Policy by employees 4. A template Appendix to the employment contract with basic terms regarding the processing of personal data of and by employees

2.2.2 Methodological framework for the generation of the sample good practice material

In this section, we present the methodological framework for the generation of suitable sample guidance documents to the SMEs based on the contextual information on the data controller. This framework is based upon the content tiles as specified in section 2.2.1 and facilitates the generation of guidance documents adaptable to each SME's particular needs. The online wizard of the toolkit contains a set of interactive questions that will guide the user (an SME) to produce the desirable guidance outcome based on the characteristics of data processing pertaining to the particular user, containing clear instructions to the SMEs, as data controllers, for further adjustment of the documents as well as hyperlinks to other template documents of the byDesign Project.

In the following lines the interactive questions of the online wizard are presented along with the guidance output depending on the responses provided by the particular SME.

Question about the sector: The purpose of the first question is the specification of the sector to which the SME belongs as a set of guidance documents is sector-specific.

1) Select the **sector** to which your Company belongs:
   a) Health
   b) Education
   c) Tourism - Hospitality
   d) Commerce (physical/electronic)
   e) Other [please specify]

Question about the data processing operations: The following set of questions is devoted to the specification by the SME of its processing operations related to management of customers and potential customers including direct marketing, management of suppliers as natural persons, management of personnel and prospective employees as well as video surveillance.

1) Do you collect and process personal data about your Company's **customers**?

2) Do you **directly promote products and services thought electronic means** (direct marketing by sending email and/or SMS) to your Company's **customers**?

3) Does your Company collect and process personal data to reach **potential customers**?

4) Does your Company have **natural persons as suppliers**?

5) Does your Company **employ employees** (under any employment relationship or work contract or independent service contract)

6) Does your Company collect and process personal data on **prospective/candidate employees**?

7) Have you installed and operate a **video surveillance system** in your Company?

The responses given by the SME to the above questions allow specifying the set of processing operations carried out by each particular SME. Based on these processing operations and the sector, as specified from the first question of the online wizard, the relevant templates for providing information to data subjects are provided to each particular SME (i.e. relevant material from section A2 of Table 1). To facilitate ease of use and better GDPR compliance, a table is also provided which contains the processing operations of the particular SME with the corresponding data processing purposes, legal bases and data subjects' rights.

Furthermore, the templates of the data subject rights exercise request forms and a simple and comprehensive guide for data subjects request handling procedures are provided to the SME (i.e. relevant material from section A4 of Table 1). In addition, the output contains the model records of those processing operations specified by the particular SME (section B1 of Table 1).

Finally, a set of FAQs is provided to the SME on transparency (section A1 of Table 1), on the processing of employees' and prospective employees' data (section C4 of Table 1), on direct marketing through electronic means to customers and potential customers (section C2 of Table 1) and on video surveillance along with a checklist with minimum requirements for the installation and operation of a video surveillance system (section C3 of Table 1).

Questions about personnel management: The set of the following questions allows the SME to further specify its needs regarding personnel management.

1) Do your Company's employees **use electronic means** in the context of their employment?

2) Is you Company interested in a **model annex template** to the contract with your employees for the processing of their personal data?

3) Is your company interested in an **awareness-raising brochure** for your employees about personal data breach incidents?

Based on the responses to the above questions the SME is provided with the following guidance documents: a template of a Use of Electronic Media Policy by employees, a template Appendix to the employment contract with basic terms regarding the processing of personal data of and by employees and an employee awareness leaflet on personal data breaches (i.e. material from section C4 of Table 1).

Question about contractors/processors: The purpose of the following set of questions is to gather the responses of the SME on the use of contractors/processors for the processing of personal data and the specific services these processors provide.

1) Do you use **contractors/processors** (natural or legal persons) for the processing of personal data on your Company's behalf?

2) Select the **service or services** provided to your Company by the contractor/processor:
   a) Accounting services
   b) Support services for IT systems
   c) Hosting and cloud provider services
   d) Product and service promotion services (marketing)

e) Physical security services
f) Other services [please specify]

According to the responses of the SME, the guidance output contains the FAQs regarding the processors and one or more templates of an appendix regarding the processing of personal data to a signed contract between the controller and the processor based on the services provided by the processor (i.e. material from section B4 of Table 1).

Questions about the website: The following set of questions allows the SME to specify the activities performed through its website.

1) Does your Company have a **website**?

2) Can visitors/users register through your Company's website for receiving your **e-newsletter**?

3) Do you **measure and analyse the use** of your Company's website by visitors/users?

4) Do you display **advertisement**s on your Company's website?

5) Do you offer visitors/users the possibility to **share the pages** of your Company's website (**share buttons)** on social media?

6) Does a **cookie window** appear on your Company's website (**cookie banner**) to inform and obtain consent for optional cookies?

Based on the above responses, the guidance output provided to the SME contains checklists of clear requirements for a business website regarding transparency, security measures and compliance with cookies (i.e. material from section C1 of Table 1).

Questions about consent: The purpose of this question is to provide the SME with FAQs about consent as a legal basis for personal data processing and templates for declaration of consent of customers/ employees/prospective employees according to the needs of the SME (i.e. material from section A3 of Table 1).

1) Is your Company interested in information on the use of **consent as a legal basis** for the processing of personal data?

2) Select the **consent declaration templates** that your Company is interested in:
   a) a template of a customer's declaration of consent for photography and video recording of an event,
   b) a template of an employee's declaration of consent on the collection of material from social events and/or promotional activities
   c) a template of an employee's declaration of consent on optional benefits,
   d) a template of a prospective employee's declaration of consent.

Questions about personal data file destruction, data breaches and security measures: Guidance documents on these three areas will be provided to the SME with a positive answer to the following question (sections A5, B2, B3 of Table 1).

1) Is your Company **interested** in the following:
    a. Information on personal data files destruction and sample templates about File Destruction Policy and File Destruction Protocol?
    b. A list of basic personal data security measures?
    c. Information and procedures for detecting and handling personal data breaches?

Optional question about Company Information: This is an optional question that allows the SME to specify its company details. In this case these details are included into the guidance documents provided to the SME.

1) **Optionally**, you can fill in your **Company details** to be included in the generated documents (this information is not stored or kept by the online Toolkit):

- Legal name
- Distinctive title
- Address (Street, Number, Area, City)
- Telephone number
- E-mail address
- If you have designated a Data Protection Officer (DPO), please fill in the contact details with the DPO (telephone, email).

3 Brief presentation–description of the sample good practice material

3.1 Transparency

3.1.1 Purpose-benefits for the SME

Transparency is one of the basic and fundamental principles of data protection within the new legal framework of GDPR, as provided in article 5. It is further analysed in recital 39 of GDPR that it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of personal data should be easily accessible and easy to understand, and that clear and plain language should be used. In essence, the obligation that transparency entails for data controllers and processors covers the provision of information to data subjects related to fair processing, how data controllers communicate with data subjects in relation to their rights under the GDPR as well as how data controllers facilitate the exercise by data subjects of their rights. Transparency, including its content and modalities is implicitly discussed in articles 12, 13 and 14 of GDPR.

Since transparency forms an obligation for data controllers and processors for which they are held accountable and in light of the difficulties they are faced with when they have to meet the transparency requirements, simplified information material in the form of FAQs is prepared, so as to assist controllers and processors in the provision of all the necessary information to data subjects in an appropriate, timely and lawful manner.

3.1.2 Description-brief analysis

The FAQs that are drawn contain information on the following:

- The concept and meaning of transparency.
- The specifications and requirements in relation to:
  - substance (content of the information and variation of content depending on the source from which the personal data originate: gathered from publicly accessible source or the data subjects themselves),
  - manner (means of providing information),
  - time for providing transparent information to data subjects – with special mention to the need for timely notification of information in cases of fundamental change to the nature of the processing operation or change that might be unexpected and surprising for the data subjects.
- The need for the specific requirements for the provision of information when data processing involves children, as a special category of data subjects.

3.2 Templates for the provision of information to data subjects

3.2.1 Purpose-benefits for the SME

According to Articles 12, 13 and 14 of the GDPR, the SME as data controller has the obligation to take appropriate measures to provide the necessary information relating to the processing of personal data to the data subject. For this purpose, the different categories of individuals whose personal data are collected and processed by the SME should be accordingly informed by the controller. These categories include the customers/clients of the SME, the potential customers, the employees, the prospective/candidate employees as well as providers (natural persons) as data subjects,

In order to address the SMEs' requirement for clear and adaptable document templates for each processing activity, as identified through the survey (D2.1), this section provides:

- A template of a document providing information to the company's customers as personal data subjects. This template has been drafted in five (5) different versions, corresponding to the business sectors of the SMEs (education, health, commerce, tourism – hospitality and other sectors).
- A template of a document providing information to the SME's potential customers.
- A template of a document providing information to the SME's employees under any employment relationship or work or independent service contract in the Company.
- A template of a document providing information to the SME's prospective/candidate employees.
- A template of a document providing information to the SME's providers - natural persons, as data subjects.
- Templates of documents providing first and second-level information to individuals on video surveillance.
- A template of a document providing information to individuals in case of a personal data breach.

3.2.2 Description-brief analysis

The templates for providing information to data subject of all categories regarding the processing of the personal data include the following:

- The identity and the contact details of the controller.
- The type(s) of personal data and their sources.
- The purposes and legal bases of the processing.
- Information on data transfer and data recipients.
- Data retention period.
- Data transfer outside E.U.
- Rights of the data subjects and how they can exercise them.

The templates are adaptable to each company's particular needs and contain clear instructions to the SMEs as controllers, as well as hyperlinks to other template documents of the Project, where needed (i.e. to the general information on data rights, and application forms to exercise them), thus forming a whole in the context of the toolkit.

3.3 Consent

3.3.1 Purpose-benefits for the SME

Consent is one of the six legal bases for data processing as listed in article 6 of the GDPR. It is essential that before the start of any processing activity, the controller considers the appropriate legal basis for each of the intended processing activities. Consent can only be an appropriate lawful basis if a data subject is offered control and has a genuine choice with regard to accepting the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.

The key points in order to ascertain whether consent is valid are also stipulated in article 4 (11) and 7 of the GDPR. The process for obtaining consent is also of the utmost importance for the data protection legislation.

In the employment relationship, consent is exceptionally chosen as the legal basis on data processing only in cases where the employer can prove that it is indeed freely provided and the provision of consent will not have any negative consequences for the employee. Such cases are for example, the processing of employees' personal data in social events, promotion of the company or for the provision of optional benefits to the employee. Thus, for the processing of those employees' data, declaration of their consent should be provided to the controller. Accordingly, candidates should also provide the controller with their choice on the data retention period.

Based on the results of the survey, it was evident that controllers were facing difficulties with determining the correct legal basis for their processing. Difficulties were also detected in relation to the means and timing of obtaining consent. In view of the above mentioned observations, it is established that SMEs could benefit from information material on the concept and meaning of consent as well as the requirements including the proper lawful ways to obtain and retain valid consent. Furthermore, in the context of compliance with the GDPR, it is very valuable for an SME to have templates of the data subject declaration of consent.

To this end, to assist controllers and processors in their decision on which cases consent is the appropriate legal basis and how to apply it, simplified information material in the form of FAQs as well as consent declaration templates are prepared. The templates are the following:

1. A template of a customer's declaration of consent for the collection of photographs and videos of a private school event.
2. A template of an employee's declaration of consent on the collection of material from social events and/or promotional activities of the company,
3. A template of an employee's declaration of consent on optional benefits.
4. A template of a candidate declaration of consent.

3.3.2 Description-brief analysis

The FAQs that are drawn contain information on:

- The concept and meaning of consent, cases when it is the appropriate legal basis and cases (including examples) when it should not be used.
- Description of the rest of the legal bases.
- Lawful ways and process for obtaining consent as well as the timing of securing consent and possible time limitation of its validity.
- Consent with regard to processing activities aimed at children.
- Consent in relation to processing activities of employees.
- Procedure for enabling data subjects to withdraw consent.
- Compliance status and lawfulness of consent acquired before the GDPR.

The templates of the customer/employee/prospective employee declaration of consent include the following necessary elements:

- The identity and the contact details of the data controller.
- The data that are going to be collected.

- The purpose and legal basis of the processing.
- The data retention period and in case of the prospective/candidate employee the choice on the data retention period.
- The option to withdraw consent.
- A brief delineation of the data subject's rights and procedure for the exercise of these rights.
- The procedure of submitting the declaration.
- The contact details and signature of the data subject.

3.4 Exercise of data protection rights and data subjects request handling procedure

3.4.1 Purpose-benefits for the SME

GDPR grants individuals, in their capacities as consumers, employees, citizens and so forth a range of specific data subject rights concerning their personal data which they can exercise under particular conditions, as per usual always, with a few exceptions. These rights which are one of the main pillars of data protection, are listed in GDPR, Chapter III, in articles 15 until 22, as article 12 on transparent information, communication and modalities for the exercise of the rights of the data subject stipulates.

In this context, GDPR compliance means enabling the exercise of these fundamental rights. Therefore, essential guidelines on how an SME should deal with the exercise of these rights by their data subject seems crucial for a fully GDPR compliance.

This section aims to provide these guidelines and assist SMEs that as data controllers have a legal obligation towards the aforementioned rights. In fact, this guide facilitates self-assistance for SMEs with a set of context-aware templates of essential information on the exercise of data subject rights. This assistance, in particular, consists in a very analytical description of every single fundamental right enshrined in GDPR, that apart from mere definitions, contains specific directions on how SMEs should deal with the data subjects requests for access to their data, rectification of inaccurate or incomplete data, portability, erasure or objecting to the processing, restriction of the processing and non-automated individual decision-making.

Furthermore, SMEs benefit from the existence of templates of data subject rights exercise request forms that may use when they handle such requests. In order to be even more helpful and disseminate additional information, FAQs regarding the exercise of data subject rights and the relevant obligations of SMEs as data controllers are also provided in this section.

3.4.2 Description-brief analysis

In this section, a simple and comprehensive guide has been provided to SMEs in order for them to manage the data subject request handling procedure and to be aware of the way they can inform and respond to customers/employees as data subjects regarding the exercise of their rights. To this end, an analytical description of every single right and the related obligations of the data controller is provided. In particular, the information given covers the following main issues:

- Definition and meaning of each right.
- Way of exercise the specific right.
- Related obligations of the SME as a controller.
- Time constraints.
- Exercise of rights by minors.

- Conditions of rejection of a request and further data subject rights.

Furthermore, a template of each data subject right exercise request form is provided to facilitate the SMEs while they handle GDPR rights requests. This detailed guide is accompanied by a simple FAQ section.

3.5 Destruction of personal data

3.5.1 Purpose-benefits for the SME

Destruction of filing systems with personal data constitutes an operation of processing (art 2. 2). As such, destruction itself shall comply with the principles of storage limitation (art.5 par. 1 e) and of integrity and confidentiality (art.5 par. 1 f), namely personal data shall not be kept and stored for no longer than is necessary for the purposes for they are processed, using appropriate technical or organizational measures to ensure appropriate security of the personal data. In order to facilitate SMEs to comply with fair and lawful destruction of filing systems with personal data, a sample template on file destruction policy, as well as a sample of a file destruction protocol is been presented, accompanied by answers to Frequently Asked Questions, enlightening the steps and principles which must be followed. Consequently, the aim of the deliverables presented is to minimize the chances of a data breach, as well as to enhance the liability of each SME.

3.5.2 Description-brief analysis

In this context, the sample template on file destruction policy provides a simplified set of guidelines that helps SMEs to destroy data in compliance with the data protection rules. Thus, either paper documents or digital files, SMEs shall destroy data by shredding, overwriting, even by using file erasers, file shredders or file pulverisers. The destruction may take place daily or regularly, depending on the period that is necessary for the purposes for which the personal data are processed. In addition, each SME shall document and justify the timeframe of the storage based on two factors: the purpose of the processing and any regulatory or legal requirements for retaining data. When SMEs choose to delegate the operation of destruction to a company/entity on their behalf (processor), they shall pay attention to the terms of contract, ensuring the steps and principles of the securely destruction are been followed. Finally, SMEs shall document the destruction in order to comply with the storage limitation principle and to demonstrate their compliance. Both the sample template on file destruction policy, as well as the file destruction protocol, along with answers to Frequently Asked Questions aim to facilitate SMEs to destroy personal data fairly and lawfully.

3.6 Records of processing activities

3.6.1 Purpose-benefits for the SME

GDPR establishes a general obligation to provide evidence and to document the legality of the processing (art. 24 par.1). GPDR also contains an explicit duty of the controller and processors to keep a record of processing activities (art. 30). Keeping records of processing activities is a form of documentation and a vital tool of data protection legislation for the implementation of the transparency obligations. Records must be kept in writing (art. 30 par. 3). It also may be required to make records available to the HDPA on request (art. 30 par. 4). Finally, records must be kept updated, in order to reflect current processing activities. The content of records of the processing activities varies upon the one who is obliged to maintain the records, namely a) the data controller and where applicable his representative (art. 30 par.1), or b) the data processor, and where applicable his representative (art. 30 par. 2). The obligation to maintain records shall not apply to an enterprise employing fewer than 250 persons, unless a) processing is likely to result in a risk to the rights and freedoms of data

subjects, or b) processing is not occasional, or c) processing includes special categories of data or personal data relating to criminal convictions and offences (art. 30 par. 5).

Taking into consideration that for many micro, small and medium sized enterprises article 30 GPDR poses a new administrative requirement, model records aim to clarify the terms and principles of the records of processing activities and assist SMEs into fulfilling their respective obligation. Therefore, this section provides model records of the core processing activities performed by SMEs. It also illustrates the process that can be followed by SMEs in order to create such records using the model records provided, in compliance with data protection rules.

3.6.2 Description-brief analysis

In this context, model records present the main operations or set of operations performed by SMEs in their duration/lifetime, as long as personal data are being processed. More specifically, in this section a template of a simplified record of processing activities is provided for each of the selected sectors of SMEs, namely Commerce, Tourism and Hospitality, Education and Health, based on seven different set of operations related to the following activities:

- Customer/client management.
- Personnel management.
- Management of prospective/candidate employees.
- Management of suppliers-natural persons.
- Use of video surveillance,
- Direct marketing to potential customers.
- Data breach management.

Each of the abovementioned templates of processing activities includes pursuant to art. 30 par. 1 and 2 GDPR information regarding the following:

- The purposes of the processing.
- A description of the categories of personal data.
- A description of the categories of data subjects.
- The categories of recipients to whom the personal data have been or will be disclosed.
- The retention period of the different categories of data.
- A general description of the technical and organisational security measures.

These templates provide instructions to the SMEs, as data controllers, on how to expand and adapt the template records of processing activities to the needs of each SME, the particular characteristics of the processing and additional processing operations that the SMEs may have.

In addition, this section provides a) simplified answers to Frequently Asked Questions that may arise by the creation of records, and b) a template, explaining the principles that must be fulfilled for a sufficient content of records of processing activities, aiming to facilitate SMEs to comply with their obligation to create and maintain records of processing activities.

3.7 Security measures of personal data

3.7.1 Purpose-benefits for the SME

One of the core obligations for all businesses, including SMEs, acting either as data controllers or data processors, in GDPR is that of the security of personal data. In particular, according to GDPR, security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).

SMEs may not be fully acquainted with the perception of risk from the personal data perspective and they could benefit from a guided approach that will bridge the gap between the legal provisions and their understanding and perception of risk. Therefore, this section provides a simple and comprehensive list of general organizational and technical security measures, suitable and adaptable to the typical processing activities of the SMEs, according to the sectors they belong to. Such a list should assist controllers to comply with their GDPR obligation for personal data security. This list presents an indicative, non-exhaustive, categorization of security measures and the respective SME should define its procedures and plans so that the measures taken are appropriate for the risks involved in the processing.

3.7.2 Description-brief analysis

In this context, the comprehensive list of general organizational and technical security measures contains the following categories:

1. Organizational security measures including security policy, training and awareness-raising of staff, management of roles and responsibilities of staff and external processors, destruction of data, document display, handling of personal data breach incidents, control procedures.
2. Technical security measures including data protection techniques (encryption, pseudonymisation, anonymization), backups, management of user accounts and passwords, management of mobile or portable devices, security of workstations (protection against malware, security updates, rights to manage programmes/applications, management of detachable media), communications security, firewall, remote access (VPN).
3. Physical security measures including physical access control, protection against natural disasters.

3.8 Data breach handling

3.8.1 Purpose-benefits for the SME

GDPR imposes on all data controllers, including SMEs, the obligation to notify in a timely manner personal data breaches to the competent supervisory Data Protection Authority and inform the affected data subjects when certain conditions are met. Therefore, the SME, as data controller, must implement appropriate technical and organizational measures with the main objective to prevent personal data breaches from occurring; in the event that such an incident takes place, it shall be detected and addressed in a timely manner. For this purpose, the SMEs must be prepared before the breach takes place and must have designed and drafted a management and response plan. The SME should be able to assess the risk of the adverse consequences for individuals as a result of a personal data breach. This will allow the SME to (a) take effective actions to contain the data breach knowing the seriousness of its consequences and (b) fulfil the obligations of the GDPR vis-à-vis the supervisory authority and the affected individuals based on the level of risk.

Due to the importance of the GDPR obligations regarding personal data breaches and the strict time limits defined in the GDPR for their fulfilment, SME will benefit from a guidance document explaining their obligations and containing information and procedures on how to identify personal data breaches and how to handle them both internally in the SME and towards the data subjects affected. Furthermore, the employees of the SME should be aware of their own responsibilities regarding data breaches as well as the responsibilities of their employer (the SME). The SMEs will benefit from keeping their personnel informed about the GDPR obligations on data breaches and the actions they should take to possibly prevent data breaches or react in a timely and organized manner in case a data breach occurs.

In this context, this section provides a guidance document for the SMEs containing information and procedures for the timely detection and proper handling of personal data breaches as well as an employee awareness leaflet.

3.8.2 Description-brief analysis

The guidance document for the SMEs containing information and procedures for the timely detection and proper handling of personal data breaches contains the following:

- Definition and types of data breaches (confidentiality, integrity, availability breach).
- Data breach management procedures (various procedures, risk assessment, measures to be taken).
- Possible consequences of the data breach and factors to be taken into account in the risk assessment.
- Analysis of the notification obligation of the SME as data controller (what it is, when it is required, the necessary information for the modification procedure).
- Analysis of the obligation of the SME to communicate the data breach to the affected individuals.
- Obligation of the SME to internally document the data breach (content of the internal record).
- *Obligations* of processors according to the GDPR.
- Typical examples of data breaches that may affect an SME.

The employee awareness leaflet on personal data breaches contains crucial information on the following issues:

- Simplified definition and types of data breaches.
- Explanation of the possible effects of a data breach on individuals.
- Explanation of the obligations of the employer (the SME) deriving from the GDPR (notification to the DPA, communication to data subjects, internal documentation).
- Typical examples of data breaches that may affect an SME.
- How can an employee detect a possible data breach incident.
- What actions the employee can take in case he/she becomes aware of a possible data breach incident.
- What steps the employee can take to protect the personal data he/she has access to from a possible data breach incident.

3.9 Assignment of data processing to contractors/processors

3.9.1 Purpose-benefits for the SME

According to article 28 of the GDPR, the data controller shall use only those processors who provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. The relationship

between the controller and the processor must be formalised by means of a binding contract or other legal act that sets out, as a minimum content, the basic obligations of the contracting parts. The same obligation also applies to processors when they subcontract processing activities with other sub-processors.

In the context of compliance with the GDPR, it is very valuable for an SME to have a template of the aforementioned contract. Therefore, this section provides:

1. A general template of an appendix regarding the processing of personal data to a signed contract between the controller and the processor that can be used by SMEs in any business sector.
2. Two instances of a template of an appendix regarding the processing of personal data to a signed contract between the controller and the processor that can be used in each case that the processor of the SME is a:
    - company that provides services of promoting products and services, and
    - a cloud provider company.

In order to be even more helpful and disseminate additional information, FAQs regarding the processors, explaining the relationship between controller and processor and the main responsibilities of processors deriving from the GDPR, are also provided in this section.

3.9.2 Description-brief analysis

The provided template of an appendix regarding the processing of personal data to a signed contract between the controller and the processor includes:

- Identity and contact details of the controller and the processor.
- Preamble with the legislation in force and the subject-matter of the contract.
- Rights and obligations of the controller.
- Obligations of the processor.
- Subject-matter, nature and purpose of the processing, the type of data, the categories of data subject whose data is processed.
- Confidentiality.
- Security of processing.
- Authorisation of subcontractors.
- Place of processing – data transfer to third countries.
- Assistance to the controller.
- Data breach notification.
- Erasure or return of the data.
- Audits.
- Entry into force of the contract.

3.10 Website data protection requirements - Transparency

3.10.1 Purpose-benefits for the SME

A business website is one of the most common activities entailing personal data processing. As found by the survey among SMEs, proper and lawful functioning of their website is one of their main concerns regarding data protection issues. It also became apparent that the preferred use of guidance should be one focusing on the obligations of the website constructors. Based on these conclusions, simplified information material in the form

of a checklist was prepared, so as to assist controllers and their respective processors (website designers, programmers etc.) to meet GDPR main requirements, regarding their website operation.

In this framework, and taking into account that transparency is one of the fundamental principles of data protection and a basic obligation for data controllers, this checklist contains a list of the key transparency requirements of the GDPR as applied on a website. Thus SMEs should have the option to either review and, if needed, adjust their existing information texts to the checklist, or create a new information text, possibly based on the information templates (3.2.2) which meets the checklist requirements.

3.10.2 Description-brief analysis

The checklist contains information on the minimum transparency requirements according to Art. 13 GDPR, as applies in the case of websites, depending on the specific processing activities of each SME as controller. SMEs as controllers are assisted by an easy-to-understand list of items which must be provided to website visitors/users as data subjects, enhanced with examples from common practice, including:

1. Information on the website owner (data controller).
2. In which cases visitors'/users' data is being processed (IP collection, contact forms, user registration forms, user profiles, etc.).
3. What kind of data is collected.
4. The purpose(s) and legal basis(-es) for the processing.
5. The recipients or categories of recipients (host provider, technical support provider, marketing/tender service provider).
6. Possible data transfers outside the EU.
7. Duration of the processing.
8. Data subjects rights and ways to exercise them.

3.11 Website data protection requirements – Security measures

3.11.1 Purpose-benefits for the SME

Nowadays, a large part of the activities of small and medium enterprises is carried out electronically or via the internet. From the data breach notifications submitted to the GDPR supervisory authorities it is clear that a large number of incidents would have been avoided if SMEs had paid more attention to their online presence and their electronic applications.

While adoption of ICT systems and the Internet has provided significant opportunities for organizations to broaden their business horizons, it has at the same time increased the risk of their exposure to cyber threats. Nowadays, cyber security represents one of the main challenges faced by IT enterprises, especially SMEs.

To increase the awareness and the knowledge of SMEs on these issues, this section provides a checklist with clear requirements on the adoption of security measures for a business website, which can be used as a way to ensure that IT companies offering website construction services respect data protection legislation. The measures detailed in the checklist, however, are only indicative and provide a minimum security baseline that may be enhanced or customized, according to the company needs.

3.11.2 Description-brief analysis

In order for website security to be thorough and comprehensive, it needs to cover both the network infrastructure as well as the applications, data bases and servers of the controller. While the first guarantees that only authorized connections are made to the company's website, the latter ensures that IT staff maintain software - in all levels (Operating System, Databases, and Applications) - in a way that doesn't impair user's data security. It is a two way approach in order to sanitize the IT environment and protect it from any potential risk being materialized, either intentionally or not, by both external and internal parties. The minimum security requirements for internet infrastructure and service (website) contain a) security measures of communication networks such as network diagram, demilitarized zone, network segmentation, monitor of network activity, use of a web application firewall etc. and b) security measures of servers, applications and databases such as Installation of the latest security updates, protection against malicious software, use of TLS protocol, use of strong passwords, secure backup of servers/applications/files, protection against SQL attacks or script injection etc.

3.12 Website data protection requirements – Cookies compliance

3.12.1 *P*urpose-benefits for the SME

Most SMEs use their website as one of the main points of presence and to keep alive the relationship with their customers. Cookies and tracking techniques are used by many websites for several activities including user authentication, maintaining the user session and the effective functioning of online services, advertising and measurement analysis, sharing of pages in social media. As found by the survey among SMEs, while SMEs are mostly aware of the cookie legislation, they cannot identify which are the correct default options in cookie settings. Based on these conclusions, simplified information material in the form of a checklist was drafted, so as to assist controllers and their respective processors (website designers, programmers etc.) to meet the requirements regarding cookies compliance.

In this context, and taking into account the widespread use of cookies and the growing concern of website visitors and users on data collected through cookies, this checklist contains a list of the key requirements for website compliance with cookies. This will assist SMEs to review and possibly adjust their existing cookie setting and serve as guidance for their processors as well.

3.12.2 Description-brief analysis

The checklist prepared contains information of the following:

1. The meaning of cookies and the provisions of the legislation.
2. Requirements in relation to consent on the use of optional cookies:
   - explanation on optional and necessary cookies,
   - manner for providing consent (positive user action, not pre-defined boxes),
   - central and user-friendly management of providing and withdrawing consent for optional cookies.
3. Transparency – conditions for informing users and visitors of the website for cookies
   - manner and time for the provision of information (easily accessible, comprehensible and structured form),
   - minimum content of the cookie policy,
   - table with information on the cookies of each category.

4. Minimum requirements for the cookie banner of the website (information contained, level of appearance of the provided options, ability to reject all optional cookies at the first-level).

3.13 Direct marketing through electronic means – e-Newsletter

3.13.1 Purpose-benefits for the SME

The terms and conditions for direct marketing, which involves the processing of personal data, are detailed in the e-privacy regulation – Directive 2002/58/EC. The basic rule being that in order to use electronic means of communication for advertising purposes, consent is needed with the exception of the case of existing customers under certain conditions.

Based on the results produced by the survey amongst SMEs, it is evident that controllers and processors encounter problems with the use of electronic means and newsletter communications for direct marketing purposes. They indicated that they need guidance on determining the legal basis for direct marketing, possible lawful ways to contact potential customers as well as existing customers, means to obtain and retain consent and guidance regarding the data subjects' right to unsubscribe. They were also interested in the proper use of social media for advertising. Therefore, simple and clear information is provided by means of FAQs addressing the deducted, existing ambiguities and main areas of interest for the SMEs. Moreover, clear instructions have been formed for sending newsletters for the purposes of direct marketing, combined with a model information text and template e-mails.

3.13.2 Description-brief analysis

The FAQs that are drawn contain information on:

- The lawfulness of communicating with existing customers (description of such cases and prerequisites).
- The lawfulness of communicating with potential customers via various sources e.g. mailing lists etc.
- Means of obtaining consent in case of potential customers and relevant information to be given at that stage.
- Content of information to be included in the advertising messages.
- Conditions for communicating with potential customers by telephone.
- Measures and steps that must be included in standard business procedures with regard to addressing requests and complaints from the recipients.
- Requirements that must be fulfilled in order to use social media accounts for direct marketing.

The Instructions for sending newsletters contain information on the legal basis of this data processing activity, the information which has to be provided to recipients, the consent procedure, data retention, security measures and other obligations of the SME as data controller.

As templates have been drafted an information text to be displayed in the registration form and three confirmation e-mails for each stage of the registration procedure.

3.14 Video surveillance

3.14.1 Purpose-benefits for the SME

According to Articles 12, 13 and 14 of the GDPR, the data controller has the obligation to take appropriate measures to provide in writing the necessary information to the data subject relating to the processing. Thus, if

a video surveillance system captures images of individuals, then personal data is being processed and the data subjects should be accordingly informed by the SME as data controller.

In the context of compliance with the GDPR, it is very valuable for an SME to have a template of the provision of information to data subjects on video surveillance. Therefore, this section provides:

1. A document describing the obligation of the SME to provide information to data subjects regarding the processing of their personal data through a video surveillance system.
2. A template of a warning sign as a first layer information with or without QR (i.e. with a QR an SME can modify the image by inserting a link to the website with the second level information, if it wants to refer to a website) and with or without the reference to a DPO.
3. A template to provide information on the processing of personal data through a video surveillance system of the SME as a second layer information.
4. A checklist with minimum requirements for an SME for the installation and operation of a video surveillance system.

In order to be even more helpful and disseminate additional information, FAQs regarding data processing through the video surveillance system, explaining the main responsibilities of the controller deriving from the GDPR, are also provided in this section.

3.14.2 Description-brief analysis

The first good practice document provides guidance to the data controllers on the obligation to inform data subjects regarding the processing of their personal data through a video surveillance system and explains what is included in the first- and the second-level information to data subjects.

The template of a warning sign, with or without using a QR code, includes the first-level information on video surveillance regarding:

- The purpose of the processing.
- The identity of the controller and/or its representative.
- The reference to the rights of the data subject.
- The contact details of the Data Protection Officer in case one has been appointed.

The template for providing information to data subjects on the processing of personal data through a video surveillance system of the SME as a second-level information includes:

- The contact details of the controller.
- The purpose of processing and legal basis.
- The data type and categories of data subjects.
- The recipients.
- The data retention time.
- The rights of data subjects.
- The right to lodge a complaint.

The checklist with the minimum requirements for the installation and operation of video surveillance system includes the following:

- The basic requirements for any business sector.

- The specific requirements for the selected business sectors i.e. health, tourism-hospitality, education and commerce.

3.15 Employee records

3.15.1 Purpose-benefits for the SME

Employee records

According to Article 30 of the GDPR, each controller shall maintain a record of processing activities under its responsibility. Among those processing activities SMEs shall have activities relating to the management of its personnel and prospective/candidate employees for which it would be very helpful for SMEs to have a template of the relevant record. Therefore, this section provides a template record relating to:

- personnel management processing activities, and
- prospective/candidate employees' management processing activities.

Contract between controller and employees and template of a Use of Electronic Media Policy by employees

According to the GDPR, the data controller has certain obligations and should provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. Thus, controller's employees need to know and to abide with those obligations as well as to be aware of their rights regarding the processing of their data. The relationship between the controller and its employees must be formalised by means of a binding contract (or an appendix to an already signed contract) or other legal act that set out, as a minimum content, the basic obligations of the parts.

In the context of compliance with the GDPR, it is very valuable for an SME to have a template of the aforementioned documents. Therefore, this section provides:

1. A general template of an appendix regarding the processing of the personal data to a contract between the controller and its employees.
2. A template of a Use of Electronic Media Policy by employees.

In order to be even more helpful, FAQs regarding employees' and candidates' data processing are also provided in this section.

3.15.2 Description-brief analysis

Employee records

The provided template of the processing activities in the records of processing activities includes for both personnel and candidates' processing activities:

- purpose of data processing,
- categories of personal data,
- categories of data subjects,
- recipients to whom the personal data have been or will be disclosed,
- data retention time,
- general description of technical and organizational measures

Contract between controller and employees

The provided template of the appendix regarding the processing of the personal data to an already signed contract between the controller and its employees includes:

- the identity and the contact details of the controller and its employee
- preamble with the legislation in force and the subject-matter of the contract,
- the type of data and the source of their origination,
- purpose and legal basis of the processing,
- data transfer – recipients,
- data retention period,
- data transfer outside E.U.,
- data rights of the employee,
- technical and organisational measures,
- data processing by the employee,
- optional terms on employee's consent

Template of a Use of Electronic Media Policy by employees

The above template includes:

- purpose
- definitions
- policy of Accepted Use of Electronic Means of Communication
- policy of Access and Control of the Electronic Means of Communications by the Company

4 Conclusions

The sample good practice material will facilitate the GDPR compliance process of Greek SMEs, by giving them useful and practical information and templates on the most crucial topics of GDPR compliance, such as the provision of information to data subjects, the consent as a legal basis for data processing, the exercise of data subjects' rights, the transparency requirements, the destruction of files containing personal data, the records of processing activities, the basic security measures, the handling of personal data breach, the assignment of data processing to contractors/processors, the website data protection requirements, the direct marketing through electronic means – e-Newsletter, and video surveillance, both at the customer and employees levels.

In this way, all the important issues and requirements of GDPR compliance will be covered and analysed.

On the basis of this work, Task 2.3 will continue the work presented in this deliverable, by facilitating the development of the online toolkit.

5 Appendix

5.1 Transparency

5.1.1 Frequently Asked Questions for the provision of information to data subjects — Transparency

1. What "transparency" means in the processing of personal data

The principle of transparency is one of the principles of the processing of personal data. Compliance with it is a prerequisite for the processing of personal data to be lawful and fair. It aims to make individuals aware that their personal data are collected, processed and used. It is essential to provide the data subject with information in order to be fully informed about the processing carried out by the controller and its rights, including how to exercise them, as well as in the event of a data breach.

2. What characteristics should the information provided to data subjects have

The information provided must be concise, comprehensible, written in a simple, clear and easily accessible form, in order to make it immediately visible to the data subject as to where he/she may find the information.

The information is provided free of charge and cannot be linked to any financial transaction (e.g. purchase of goods).

It must be in Greek and only cumulatively in another language, understood by the average recipient, and in particular by persons with slight difficulty in reading due to age, low level of education or with a mother tongue other than Greek.

Misleading concepts and expressions, legal terminology, foreign language and vague terms (such as "may", "often", "possible") and unnecessary over-information should also be avoided.

3. I have a business/website that targets/has products and/or services for children. Does the information I have to provide differ?

When the controller aims to provide goods or services to children, it is required to provide information on the processing of their personal data in clear and simple language, especially child-friendly or in a medium that children can easily understand, such as videos with cartoons, sketches with images, etc.

4. When do I have to inform subjects about the processing of their data?

In three different time circumstances, information to the data subjects should be provided.

- Before or at the start of the processing of data, i.e. where personal data are collected either by the data subject or by third parties. In particular, when collected by the subject, the information shall be provided at the stage of receipt of the data.
  When collected from third parties (including publicly available sources), the GDPR stipulates that the information shall take place within a reasonable period of time from the collection of personal data, but at the latest within one (1) month.
  If, however, the personal data are used for communication, the information is provided at the latest at the time of the first communication regardless of the fact that the month has not expired, without, however, negating the rule of a maximum time limit of one month.
  If the data are to be communicated to another recipient, the information shall be provided at the latest on the first notification and with the above mentioned final deadline of one month.

- Throughout the processing period, i.e. in any communication with data subjects about their rights.
- At specific points while the processing is ongoing, such as when a data breach occurs (and data subjects have to be informed without delay) or in case of substantial changes to the processing (such are considered to be a change in the purpose of the processing or in the identity of the controller or in the way in which data subjects can exercise their rights and not spelling errors or grammatical errors).

5. What information should be included in the information to data subjects?

- Identity and contact details of the controller.
- Contact details of the Data Protection Officer (DPO).
- Processing purposes — legal basis
    - The legitimate interests pursued by the controller or third party if the legal basis is 6(1)(f).
    - If the legal basis is consent, the right to withdraw it (without prejudice to the processing until then).
- Recipients or categories of recipients (for all — whether they are public services, third parties — other controllers).
- Intention to transfer to a non-EU country or international organisation.
- Data retention period (or criteria for determining it).
- The rights of the subject and how to exercise them, including the right to lodge a complaint with a supervisory authority.
- Whether there is a legal or contractual obligation to provide the information or a requirement to enter into a contract and whether the data subject is obliged to provide the data and what the consequences of not providing the data are.
- Key elements of the logic of any automated decision-making and profiling, the significance and foreseeable consequences for the subject.

6. I have collected personal data from publicly accessible sources/other subjects — customers/other controllers (businesses etc.). Is the information I owe the same as that which I would have provided if I collected the data from the subjects themselves?

The information described above generally applies and is mandatory in this case, and additional information is provided on:

- The categories of data.
- Their sources of origin and (if applicable) whether the data originated from publicly accessible sources.

7. How can I inform data subjects?

In writing, in text or by other means, including, where appropriate, electronically, as well as by sending an e-mail. Especially where the controller maintains a website on the internet, it is appropriate that the information is made electronically, on its website, to which the controller will refer when collecting the data.

Where the controller does not have a website, it may provide the information by means of a document (e.g. a brochure), which is handed over to the subject at the time of receipt of the data when it is done directly by the subject or sent to him/her by post in any other case. Information can also be provided by telephone contacting

a natural person or even through automated or pre-recorded information and with the possibility for more and more detailed information.

Furthermore, it may also be provided orally when requested by the data subject, provided that the data subject has been identified in advance.

In any case, the method of providing the information must be clearly visible, comprehensible and legible and generally large texts should be avoided.

Also, in cases where the subject maintains a digital account on the controller's website, the 'Privacy Tables', i.e. a specific point of management of users' preferences for the protection of personal data, may be used in order to allow or even block the use of their data in certain ways.

A good practice is a multi-layer approach to provide transparency information. Instead of providing a large, aggregated and possibly tedious text, reference should be made to different categories of information. The first level (i.e. at the first contact — cooperation between the controller and the data subject) generally provides the most important information, such as the purposes of the processing, the identity of the controller and the existence of the rights of the data subject, while detailed and specific information may be provided at other levels. At the same time, at the first level, clear instructions are given to identify the points — other levels with further information.

8. How is the multi-level information done?

Multi-level information can be carried out using the following methods:

- pop-ups (on a website)
- providing information at the appropriate point (just-in-time), i.e. where it relates to a specific action, which the subject intends to take, in order to receive appropriate and specific information (e.g. when he/she buys a product from an online business and is required to communicate his/her phone, then he/she could be informed about the purpose of collecting and keeping such data)
- icons
- cartoons
- video (on website)
- graphic representation — graph.

9. What should the controller do in case of due information due to changes in the processing?

If the characteristics of the processing significantly change, the controller must immediately inform the data subjects so that they have a reasonable time to react if they consider it appropriate (e.g. to withdraw any consent or object to the processing).

The information should be done in the most appropriate way, such as e-mail, paper letter, pop-up on a website or in any other appropriate way, so that data subjects are immediately and fully informed of these changes.

5.2 Templates for the provision of information to data subjects

5.2.1 Template for the provision of information to customers – Health sector

INFORMATION TO CUSTOMERS OF THE COMPANY

.....

ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

The company bearing the name[1]..... (and distinctive title[2].....) established in..... (street....., tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, their time of retention, their transfer outside the EU and your rights in relation to your data as customers of the Company and how you can exercise them.

B. Type of data and sources

The personal data collected and processed by the Company refer to its patients-clients, adults and minors, and are[3]:

1. Your identification and pricing details, full name, date of birth, Social Security number, Tax Identification Number and Tax Office.

2. Your contact details, postal and e-mail address, telephone number (landline, mobile).

3. Payment details, credit cards, redemptions/debts.

4. Health data (medical history, dates of visit, type of service provided, treatment, insurance capacity, details of any private insurance, etc.)

5. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

The above personal data is provided to the Company directly by our clients (you), as data subjects, and if they are minors or are under judicial assistance, by their legal representatives. The provision of your data is your legal obligation and a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide them. In addition to your medical history, your health data (under point 4 above) as well as your payment and debt information arise during the course of your transaction relationship with the Company and are retained by it.

C. Purposes and legal basis for processing

[1] Complete full legal name or first and last name in case of sole proprietorship.
[2] Fill in the distinguishing title (commercial name) of the undertaking, if any.
[3] The information mentioned is indicative and each Controller should check what is applicable to his/her case.

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

1) Provision of health services

The aforementioned personal data are processed for the purpose of providing health services[4] to you, including your identification, communication with you, etc. and the legal basis for their processing is the performance of the contract between us, in accordance with Article 6(1)(b) GDPR. As regards your health data under point 4 of Section B., the legal basis for the processing is that of Article 9(2)(h) GDPR, i.e. the fact that the processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, health or social care or treatment under a contract with a health professional, who is subject to the obligation of professional secrecy[5].

2) Invoicing of services

The data under points 1, 2 and 3 above of Section B. relating to your payments as appropriate are further processed for the purpose of invoicing the Company's services and the legal basis for their processing is the fulfilment of the Company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

3) Direct promotion by electronic means[6]

Your electronic contact details are used for the purpose of promoting similar services by electronic means (e-mail/sms), based on the overriding legitimate interest of our company in the direct marketing of its services (art. 6(1)(f) GDPR and 11(3) of Law 3471/2006).

[insert any other legitimate purposes with an indication of the appropriate legal basis. Attention to special categories of data (art. 9-10 GDPR).]

D. Transfer of data – Recipients

In order for the Company to fulfil the above mentioned functions and its related obligations, it communicates the personal data of its customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

1. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- accounting service providers: company.....[7],
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

[4] Where appropriate specialization (e.g. based on Business Activity Code Number).
[5] It can be specified according to the sector, by which provision the HR is bound by (e.g. a Code of Conduct).
[6] If you advertise by electronic means to customers, keep what is applicable.
[7] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

subject to the confidentiality of your data.

2. Financial institutions, to the extent necessary for the execution of the transaction

3. Insurance companies, to cover the insurance case

4. Social security institutions and tax authorities, in accordance with the applicable insurance and tax legislation respectively

5. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

6. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

7. [insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time interval]:

Your data is kept by the Company for [specify period] on the basis of [specify the specific provision of law][8]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

Your data is kept by the Company throughout the period of the provision of its services to you and until [specify the criteria that determine the period of compliance such as the expiry of the limitation period of the claims concerned] [9]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the operation].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transmission], with legal basis.....[insert specific legal basis] and if

[8] For example, ten (10) years since your last visit, in accordance with the Code of Medical Ethics. To be completed on a case-by-case basis by data category, based on any specific legislation (insurance, tax, etc.)
[9] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transfer]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and request form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a KEP or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Provision of health services (identification and communication details)	Performance of a contract (Article 6.1b GDPR)	Access (art. 15 GDPR) Rectification (art. 16) Erasure (art. 17) Restriction (art. 18) Portability (art 20)
Provision of health services (health data)	Contract with a health professional bound by secrecy (9.2h)	Access (15) Rectification (16) Erasure (17)

		Restriction (18) Portability (20)
Pricing of services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
Promotion of services to customers by electronic means[10]	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)

Please note that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to lodge a complaint with the Personal Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[11] of our Company, at: Tel....., Email……

5.2.2 Template for the provision of information to customers – Education sector

INFORMATION TO CUSTOMERS OF THE COMPANY

.....

FOR THE PROCESSING OF PERSONAL DATA

A. Controller's information

The company bearing the name[12]..... (and distinctive title[13].....) based in..... (street....., number. …… tel..... e-mail: .....),

[10] As long as you advertise by electronic means to customers.

[11] If there is a DPO.

[12] *Fill in full legal name or first and last name in case of sole proprietorship.*

[13] *Fill in the distinctive title (commercial name) of the company, if any.*

(hereinafter referred to as **"company**") hereby informs you, as controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, the time of their retention, their transfer outside the EU and your rights in relation to your data as potential customers of the Company and how you can exercise them.

B. Type of data and sources of origin

The personal data collected and processed by the Company refer to the pupils and, where applicable, their parents/guardians, if the students are minors and are[14]:

1. Identification and pricing details, pupil's name, father's name, mother's name, date of birth, gender, home address, tax identification number and tax office.

2. Your contact details, postal and e-mail address, telephone number (landline, mobile).

3. Payment details, credit cards, redemptions/debts.

4. Health data, personal pupil health card information.

5. Study and conduct details, scores, absences, learning difficulties, conduct, penalties, and other information included in the pupil register.

6. **Audio-visual material** (photos, videos) of the student in the context of educational, cultural, sports or other activities of the Company (events, excursions, etc.).

7. [add any other data you process (e.g. solemn declarations of parents/guardians, certificates, registration titles, etc.) if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for this purpose]

The above personal data under points 1, 2, 3 and 4 are provided to the Company directly by our clients (you), as data subjects, and if they are minors, by their legal representatives.
The provision of your data is your legal obligation and a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide it. The information on attendance and conduct (point 5 above) as well as your payment and debt information shall be obtained during the course of your transaction relationship with the Company and shall be retained by it. Images of pupils taken in the context of photography or video recording are collected on a voluntary basis only if you give your consent.

C. Purposes and legal basis for processing

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

4) Provision of educational services

[14] The information mentioned is indicative and each Controller should check what is applicable to his/her case.

The above personal data are processed for the purpose of providing educational services.....[15] to you (or your represented minor student), including your identification, communication with you, etc. and the legal basis for their processing is the performance of the contract between us, in accordance with Article 6(1)(b) GDPR. The legal basis for the processing of the student register information (point 5 above) and the identification and contact details of pupils and parents/guardians as appropriate (points 1 and 2) is the fulfilment of our company's legal obligations under educational legislation[16] (Article 6(1)(c) GDPR). As regards health data (under point 4), the legal basis for their processing is that of Article 9(2)(b) GDPR, i.e. the fact that the processing is necessary to fulfil the obligations of our company in the field of social protection, in accordance with the legislation regulated by the Student Individual Health Bulletin.

5) Invoicing of services

The data under points 1, 2 and 3 above of Section B. relating to your payments as appropriate are further processed for the purpose of pricing the Company's services and the legal basis for their processing is the fulfilment of the Company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

6) Direct promotion by electronic means [17]

Your electronic contact details are used for the purpose of promoting similar services by electronic means (e-mail/sms), based on the company's overriding legitimate interest in the direct marketing of its services (art. 6(1)(f) GDPR and 11(3) of Law 3471/2006).

7) Taking photos of students/filming events

The pupils' facial image is collected through photography or video recording in the context of educational, cultural, sports etc. activities of the Company on an optional basis, only if you give your consent, which is the legal basis for processing in this case (art. 6 (1) (a) GDPR). Consent is given upon detailed and specific information each time.

[Insert any other legitimate purposes with an indication of the appropriate legal basis. Attention to special categories of data (Articles 9-10 GDPR).]

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it communicates the personal data of its customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

8. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- accounting service providers: company.....[18],
- providers of IT support services: company.....,

[15] Be specific where appropriate (e.g. based on Business Activity Code Number).
[16] If applicable to the Company, and indicating the special provision, as appropriate.
[17] If you advertise by electronic means to customers, keep what is applicable.
[18] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

- providers of hosting services, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

subject to the confidentiality of your data.

9. Financial institutions, to the extent necessary for the execution of the transaction

10. Tax authorities, in accordance with applicable tax legislation

11. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

12. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

13. [Insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time interval]:

As part of your cooperation with the Company, your data will be retained for as long as you retain the status of a customer of the Company, and after termination for any reason of your contract for [specify period of time] on the basis of [specify the specific provision of law].[19]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

As part of your cooperation with the Company, your data will be kept for as long as you retain the status of client of the Company, and after termination for any reason of your contract until [specify the criteria that determine the period of compliance such as the expiry of the limitation period of the relevant claims] [20]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time frames, your personal data will be erased/destroyed [based on the destruction policy of the operation]

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[19] To be completed on a case-by-case basis by data category, on the basis of any specific legislation (insurance, tax, etc.).
[20] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of the following conditions is met at the same time [the Undertaking should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transmission]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and request form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, for the purpose of making the check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Centre (KEP) or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Provision of training services to customers (identification and communication details)	Performance of a contract (Article 6.1b GDPR)	Access (Article 15 GDPR) Rectification (16) Erasure (17) Restriction (18) Portability (20)

Provision of training services to clients of study/performance data)	Compliance with a legal obligation (6.1c) based on a specific provision of educational legislation as appropriate	Access (15) Rectification (16) Restriction (18)
Keep an individual pupil health card (ADYM)	Compliance with a legal obligation in the field of social protection (9.2b)	Access (15) Rectification (16) Restriction (18)
Pricing of services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
Photo shooting of students/videos of events	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Promotion of services to customers by electronic means[21]	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)

It is noted that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

[21] As long as you advertise by electronic means to customers.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to file a complaint to the Personal Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data[22], please contact the Data Protection Officer of our company, at: Tel.....Email……

5.2.3 Template for the provision of information to customers – Tourism-Hospitality sector

INFORMATION TO CUSTOMERS OF THE COMPANY

.....

ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

The company bearing the name[23]..... (and distinctive title[24].....) established in..... (street....., tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, their time of retention, their transmission outside the EU and your rights in relation to your data as customers of the Company and how you can exercise them.

B. Type of data and sources

The personal data collected and processed by the Company refer to its clients, adults and minors, and are[25]:

1. Identification and pricing details, full name, father's name, mother's name, gender, date of birth, Tax Identification Number, ID number/passport number.

2. Your contact details, postal and e-mail address, telephone number (landline, mobile).

3. Payment details, credit cards, redemptions/debts.

4. Reservation details, dates, type of reservation, any special preferences, etc.

5. Health data (e.g. any allergies, disabilities) **and preferences** (e.g. any dietary preferences), if applicable.

6. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

[22] If there is a DPO.
[23] Complete full legal name or first and last name in case of sole proprietorship.
[24] Fill in the distinguishing title (commercial name) of the company, if any.
[25] The information mentioned is indicative and each Controller should check what is applicable to his/her case.

The personal data referred to in points 1-4 above are provided to the Company directly by our customers (you), as data subjects. The provision of your data is a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide them. Your repayments and debts information arises during the course of your transaction relationship with the Company and is maintained by it. The provision of the data under point 5 above is not mandatory and any refusal to provide them results in the absence of specialized services (e.g. special diets).

C. Purposes and legal basis for processing

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

8) Provision of hotel and tourism services

The aforementioned personal data are processed for the purpose of providing tourist/hotel services[26] to you, including your identification, communication with you, etc. The legal basis for the processing of your identification, communication and booking data is the performance of the contract between us, in accordance with Article 6(1)(b) GDPR. If you provide us with special categories of data, such as health data (any allergies, disabilities, nutritional preferences, etc.), the legal basis for the processing is your consent, in accordance[27]with Article 9(2)(a) GDPR.

9) Invoicing of services

The data under points 1, 2 and 3 above of Section B. relating to your payments as appropriate are further processed for the purpose of invoicing the Company's services and the legal basis for their processing is the fulfilment of the Company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

10) Direct promotion by electronic means [28]

Your electronic contact details are used for the purpose of promoting similar services by electronic means (e-mail/sms), based on the overriding legitimate interest of our company in the direct marketing of its services (art. 6(1)(f) GDPR and 11(3) of Law 3471/2006).

[insert any other legitimate purposes with an indication of the appropriate legal basis. Attention to special categories of data (art. 9-10 GDPR).]

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it communicates the personal data of its customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

14. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

[26] Be specific where appropriate (e.g. based on Business Activity Code Number).
[27] Attention, this should be provided by means of a special form.
[28] If you advertise by electronic means to customers, keep what is applicable.

- accounting service providers: company.....29,
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

subject to the confidentiality of your data.

15. Financial institutions, to the extent necessary for the execution of the transaction

16. Tax authorities, in accordance with applicable tax legislation

17. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

18. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as audit/supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

19. [insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time frame]:

Your data is kept by the Company for [specify period] on the basis of [specify the specific provision of law][30]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

Your data is kept by the Company throughout the period of the provision of its services to you and until [specify the criteria that determine the period of compliance such as the expiry of the limitation period of the claims concerned] [31]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the company].

F. Transfer of data outside the EU

[29] If you wish to indicate only the categories of recipients, the information should be as specific as possible.
[30] To be completed on a case-by-case basis by data category, based on any specific legislation (insurance, tax, etc.)
[31] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to…… [insert company details and the country in which it is established] to fulfil its purpose…….. [insert specific purpose of transfer], with legal basis…….[insert specific legal basis] and if one of the following conditions is met at the same time [the company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transfer]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Centre or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS

Provision of hotel and tourism services to customers in general (in terms of simple data, e.g. identification and contact details)	Performance of a contract (Article 6.1b GDPR)	Access (Article 15 GDPR) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Provision of hotel and tourist services (with regard to any health data, e.g. food and accommodation preferences, etc.)	Consent (9.2a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Pricing of products/services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
Promotion of products/services to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)

It is noted that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to lodge a complaint with the Hellenic Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Office[32]r of our company, at: Tel.....Email…….

[32] If there is a DPO.

5.2.4 Template for the provision of information to customers – Commerce sector

INFORMATION TO CUSTOMERS OF THE COMPANY

.....

ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

The company bearing the name[33]..... (and distinctive title[34].....) established in..... (street....., tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, their time of retention, their transfer outside the EU and your rights in relation to your data as customers of the Company and how you can exercise them.

B. Type of data and sources

The personal data collected and processed by the Company are[35]:

1. Your identification and pricing details, name, Tax Identification Number and Tax Office.

2. Your contact details, i.e. postal and e-mail address, telephone number (landline, mobile).

3. Payment details, credit cards, redemptions/debts.

4. Transaction data, transaction history, etc.

5. Information about your participation in our customer loyalty program (loyalty/bonus), i.e. transaction points, cash out history, etc., if you participate in it.

6. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for this purpose]

The above personal data under points 1, 2 and 3 are provided to the Company by you, and, where applicable, are a requirement for the conclusion and performance of the contract between us (e.g. ordering and sending products to your home address), which will not be possible if you refuse to provide them. The provision of your data related to our customer loyalty program is optional and any refusal to provide it results in your non-participation in the program. The transaction details, your payment and debt information and any details of your participation in the loyalty program of our clients are obtained during the development of your trading relationship with the Company and are maintained by it.

C. Purposes and legal basis for processing

[33] Complete full legal name or first and last name in case of sole proprietorship.
[34] Fill in the distinguishing title (commercial name) of the company, if any.
[35] The information mentioned is indicative and each Controller should check what is applicable to his/her case.

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

11) Supply of retail trade services of products including distance e-shop services.

The data under points 1, 2 and 3 above of Section B. for your identification and communication with you are processed for the purpose of marketing products.....[36] to you in accordance with your order and the legal basis for processing them is the performance of the contract between us (performance of payment, information on orders, delivery of products, etc.), in accordance with Article 6 (1) (b) GDPR.

12) Invoicing of products

The data under points 1, 2 and 3 above of Section B. relating to your payments as appropriate are further processed for the purpose of pricing the company's products and the legal basis for their processing is the fulfilment of the Company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

13) Participation in the customer loyalty program (loyalty/bonus)

In case you participate in our loyalty program, the purpose of processing your data under points 1, 2 and 4 above is your reward with points according to the program and the legal basis for the processing is your consent pursuant to Article 6(1)(a) GDPR.

14) Direct promotion by electronic means[37]

Your electronic contact details are also used for the purpose of promoting similar products by electronic means (e-mail/sms), with a legal basis for processing the overriding legitimate interest of our company in the direct marketing of its products (art. 6 (1) (f) GDPR and 11(3) of Law 3471/2006).

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it communicates the personal data of its customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

20. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- accounting service providers: company.....[38],
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,

[36] Where appropriate specialization (e.g. based on SMR).
[37] If you advertise by electronic means to customers, keep what is applicable.
[38] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

- [insert any other category of providers]

subject to the confidentiality of your data.

21. Financial institutions, to the extent necessary for the execution of the transaction

22. Tax authorities, in accordance with applicable tax legislation

23. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

24. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

25. [insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time interval]:

Your data as a customer of the Company is retained after the completion of the transaction for [specify period of time] on the basis of [specify the specific provision of law].[39]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

Your data as a customer of the Company is kept until [specify the criteria determining the period of retention such as the expiry of the limitation period of the claims concerned] [40]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the operation].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of

[39] To be completed on a case-by-case basis by data category, on the basis of any specific legislation (insurance, tax, etc.).
[40] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

the following conditions is met at the same time [the Undertaking should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transfer]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, for the purpose of making the check of your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Services Center (KEP) or a police authority.

PURPOSE OF PROCESSING	LEGAL BASIS	RIGHTS
Supply of retail trade services of products including distance e-shop services (identification and communication data)	Performance of a contract (Article 6.1b GDPR)	Access (Article 15 GDPR) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Pricing of products	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)

Promotion of products to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)
Optional participation in a customer loyalty program (loyalty/bonus)	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

Please note that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to file a complaint to the Hellenic Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[41] of our company, at: Tel..... Email……..

5.2.5 Template for the provision of information to customers – Other sector

INFORMATION TO CUSTOMERS OF COMPANY

……

ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

The company bearing the name[42]..... (and distinctive title[43].....) established in..... (street....., tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal

[41] If there is a DPO.
[42] Complete full legal name or first or last name in case of sole proprietorship.
[43] Fill in the distinguishing title (commercial name) of the undertaking, if any.

data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, their time of retention, their transfer outside the EU and your rights in relation to your data as customers of the Company and how you can exercise them.

B. Type of data and sources of origin

The personal data collected and processed by the Company are[44]:

1. Your identification and invoicing details, name, Tax Identification number and tax office.

2. Your contact details, postal and e-mail address, telephone number (landline, mobile).

3. Payment details, credit cards, redemptions/debts.

4. Transaction data, transaction history, etc.

5. Information about your participation in our customer loyalty program (loyalty/bonus), i.e. transaction points, cash out history, etc., if you participate in it.[45]

6. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

The above personal data under points 1, 2 and 3 are provided to the Company by you, and, where applicable, are a requirement for the conclusion and performance of the contract between us (e.g. ordering and sending products to your home address), which will not be possible if you refuse to provide them. The provision of your data related to our customer loyalty program is optional and any refusal to provide it results in your non-participation in the program. The transaction details, your payment and debt information and any details of your participation in the loyalty program of our clients are obtained during the development of your trading relationship with the Company and are maintained by it.

C. Purposes and legal basis for processing

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

15) Provision of products/services

The data under points 1, 2 and 3 above of Section B. for your identification and communication with you are processed for the purpose of providing the services/products.....[46] to you in accordance with your order and the legal basis for processing them is the performance of the contract between us (performance of payment, information on orders, delivery of products, etc.), in accordance with Article 6(1)(b) GDPR.

16) Invoicing of products/services

[44] The information mentioned is indicative and each Controller should check what is applicable to his/her case.
[45] It shall be maintained if applicable.
[46] Where appropriate specialization (e.g. based on Business Activity Code Number).

The data under points 1, 2 and 3 above of Section B. relating to your payments as appropriate are further processed for the purpose of invoicing the services/products of the Company and the legal basis for their processing is the fulfilment of the Company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

17) Participation in the award programm

In case you participate in our loyalty program, the purpose of processing your data under points 1, 2 and 4 above is your reward with points according to the program and the legal basis for the processing is your consent pursuant to Article 6(1)(a) GDPR.

18) Direct promotion by electronic means[47]

Your electronic contact details are also used for the purpose of promoting our similar [products/services] by electronic means (e-mail/sms), with a legal basis for processing the overriding legitimate interest of our company in the direct marketing of its [products/services] (Article. 6(1)(f) GDPR and 11(3) of Law 3471/2006).

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it communicates the personal data of its customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

26. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- accounting service providers: company.....48,
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

subject to the confidentiality of your data.

27. Financial institutions, to the extent necessary for the execution of the transaction

28. Tax authorities, in accordance with applicable tax legislation

29. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

[47] If you advertise by electronic means to customers, keep what is applicable.
[48] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

30. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

31. [insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time frame]:

Your data as a customer of the Company is retained after the completion of the transaction for [specify period of time] on the basis of [specify the specific provision of law].[49]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

Your data as a customer of the Company is kept until [specify the criteria determining the period of retention such as the expiry of the limitation period of the claims concerned] [50]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the operation].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

[49] To be completed on a case-by-case basis by data category, on the basis of any specific legislation (insurance, tax, etc.).
[50] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transfer]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and request form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, for the purpose of making the check of your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Centre or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Provision of products or services to customers in general (identification and communication details)	Performance of a contract (Article 6.1b GDPR)	Access (Article 15 GDPR) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Pricing of products/services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
Promotion of products/services to customers by electronic means[51]	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)

[51] As long as you advertise by electronic means to customers.

Optional participation in a customer loyalty program (loyalty/bonus)[52]	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

It is noted that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to file a complaint to the Hellenic Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[53] of our company, at: Tel.....Email…….

5.2.6 Template for the provision of information to suppliers – natural persons

INFORMATION TO SUPPLIERS OF THE COMPANY

.....

ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

The company bearing the name[54]..... (and distinctive title[55].....) established in..... (street....., tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, their time of retention, their transfer outside the EU and your rights in relation to your data as the Company's Suppliers and how you can exercise them.

B. Type of data and sources

[52] It shall be maintained if applicable.
[53] If there is a DPO.
[54] Complete full legal name or first and last name in case of sole proprietorship.
[55] Fill in the distinguishing title (commercial name) of the company, if any.

The personal data collected and processed by the Company are[56]:

1. **Your identification details** (name, VAT number)

2. Your contact details, i.e. postal and e-mail address, telephone number (landline, mobile)

3. Transaction history (payments, debts, etc.).

4. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

The personal data referred to in points 1 and 2 above are provided to the Company directly by our suppliers (you), as data subjects. The provision of your data is a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide them. Payment and debt information arises during the course of your transaction relationship with the Company and is maintained by it.

C. Purposes and legal basis for processing

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

1) Supply of products/services..... by you to the Company

The purpose of the processing of your identification and communication data under points 1 and 2 is the management of the contractual relationship between us and the legal basis for the processing of these data is the performance of the contract between us, in accordance with Article 6(1)(b) GDPR.

2) Fulfilment of tax obligations

Furthermore, the purpose of the processing of your data is to keep the legally necessary documents and declarations concerning our suppliers. The legal basis for the processing of your tax data and transaction data (invoices, payments, etc.) is the fulfilment of our company's legal obligations under tax law, in accordance with Article 6(1)(c) GDPR.

[Insert any other legitimate purposes with an indication of the appropriate legal basis. Attention to special categories of data (Articles 9-10 GDPR).]

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it communicates the personal data of its Suppliers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks and the provision of the services they have undertaken to the Company. These categories are as follows:

[56] The information mentioned is indicative and each Controller should check what is applicable to his/her case.

32. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- accounting service providers: company.....[57],
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

subject to the confidentiality of your data.

33. Financial institutions, to the extent necessary for the execution of payments

34. Tax authorities, in accordance with applicable tax legislation

35. Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

36. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory/audit authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

37. [insert any other legitimate addressees]

E. Data retention time

Option A [specify a specific time frame]:

In the context of your concluded cooperation agreement with the Company, your data will be kept for as long as you remain a Vendor of the Company, and after termination for any reason for your cooperation with the Company for [specify period of time] on the basis of [specify the specific provision of law][58]

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

In the context of your concluded cooperation agreement with the Company, your data will be kept for as long as you retain the status of Vendor of the Company, and after termination for any reason for your cooperation with the Company until [specify the criteria determining the period of compliance such as the expiry of the limitation period of the relevant claims] [59]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

[57] If you wish to indicate only the categories of recipients, the information should be as specific as possible.
[58] For example, ten (10) years since your last visit, in accordance with the Code of Medical Ethics. To be completed on a case-by-case basis by data category, based on any specific legislation (insurance, tax, etc.)
[59] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

After the expiry of the above time frames, your personal data will be erased/destroyed [on the basis of the destruction policy of the operation].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs then the purposes and addressees must be indicated as follows:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the company, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any further transfer]

G. What rights do you have in relation to your data and how to exercise them

As clients of the Company you have a number of rights, in accordance with the provisions of Articles 15-22 of the GDPR, in relation to your personal data, which are processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a KEP or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Supply of products/services to the Company	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Fulfilment of tax obligations	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Erasure (17) Restriction (18)

It is noted that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you have the possibility to lodge a complaint with the Hellenic Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[60] of our company, at: Tel..... Email……

5.2.7 Template for the provision of information to potential customers

INFORMATION ON THE PROCESSING OF PERSONAL DATA
IN THE CONTEXT OF COMPANY'S DIRECT MARKETING
……

A. Controller's information

The company bearing the name[61]..... (and distinctive title[62].....) based in..... (street....., number. …… tel..... e-mail: .....), (hereinafter referred to as **"company**") hereby informs you, as data controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the

[60] If there is a DPO.
[61] Fill in full legal name or first and last name in case of sole proprietorship.
[62] Fill in the distinctive title (commercial name) of the company, if any.

protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, the time of their retention, their transmission outside the EU and your rights in relation to your data as potential customers of the Company and how you can exercise them.

B. Type of data and sources

The personal data collected and processed by our Company are your name and your electronic contact details, i.e. your email address (e-mail) [and your mobile phone number[63]]. This data is provided to the Company directly by you, as data subjects. The provision of your data is not mandatory, and any refusal to provide it will result to not receive promotional messages from our Company.

C. Purpose and legal basis for processing

The purpose of processing your above data is to directly promote our [products/services] to you by electronic means, i.e. the sending of advertising electronic messages (e-mail/sms) including the sending of newsletters. The legal basis for the processing of your data is your consent, in accordance with Articles 6(1)(a) GDPR and 11(1) of Law 3471/2006.

D. Transfer of data – Recipients

In order for the Company to fulfil the aforementioned functions and its related obligations, it discloses the personal data of its potential customers to categories of persons or bodies (recipients). The recipients have access only to those of your Personal Data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken to the Company. These categories are as follows:

38. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are

- the company.....,[64] which provides promotion services on behalf of the Company and processes the data of its potential customers for the purpose of direct advertising,
- providers of IT support services: company.....,
- providers of hosting services, cloud providers: company.....,
- **[insert any other category of providers]**

under condition of keeping the confidentiality of your data

- Lawyers, in so far as this is necessary for the exercise of the rights of the Company and the protection of its legitimate interests

[63] In case you are conducting direct promotion via sms.
[64] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

- Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as audit/supervisory authorities, if this is required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

E. Data retention time

In the context of sending marketing messages by electronic means to you by the Company, your data is kept for as long as your consent to receive such messages is into force until it is revoked or until you exercise your right to object.

If, by the end of the above period, there are ongoing judicial proceedings involving the Company and involving you directly or indirectly, the time limit for keeping your data shall be extended until a final judgment is issued.

After the above period, your personal data will be erased/destroyed [on the basis of the destruction policy of the company].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs, then, in the information, the purposes and recipients must be indicated as follows, otherwise the following are erased:]

The Company transfers to..... [insert company details and the country in which it is established] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Controller is obliged to inform accordingly of any new transfer]

G. What rights do you have in relation to your data and how to exercise them

As data subjects, you have a number of rights, in accordance with the provisions of Articles 15-22 GDPR, to your personal data processed by the Company.

The table below lists your rights based on the purpose of the processing and a corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, for the purpose of making the check of your id, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Center (KEP) or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Electronic promotion of products/services	Consent (Art. 6.1a GDPR + L.3471/2006 Art. 11.1)	Withdrawal of consent (Article 7.3 GDPR) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

It is noted that the Company has the right in any event to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you can file a complaint to the Hellenic Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, you can contact the Data Protection Officer[65] of our company, at: Tel.....Email…….

5.2.8 Template for the provision of information to employees

INFORMATION TO COMPANY WORKERS

[65] If there is a DPO.

ON THE PROCESSING OF PERSONAL DATA

.....

A. Controller's details

The company bearing the name[66]..... (and distinctive title[67].....) based in..... (street....., number. …… tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, the time of their retention, their transfer outside the EU and your rights in relation to your data as potential customers of the Company and how you can exercise them.
Workers, for the purposes of this Decision, shall mean employees under any employment relationship or work or independent service contract in the Company.

B. Type of data and sources of origin

The personal data collected and processed by the Company are[68]:

1. Your identification details, i.e. full name, father's name and mother's name, ID number, tax identification number and tax office, social security number, gender, nationality, date and place of birth

2. Your contact details, postal and e-mail address, telephone number (landline, mobile)

3. Employee's individual, family and employment status and data of your dependents (name and date of birth) to the extent necessary to fulfil the Company's statutory obligations towards you, such as granting of leave, payment of any allowances, processing of salaries and insurance obligations.

4. Data on your professional skills and qualifications, as well as your professional development in the company, i.e. CV, copies of diplomas, prior experience, professional certifications, work permits, registration number of professional bodies, certificate of fulfilment of military obligations, letters of recommendation and certificates of previous employers' experience, evaluations, productivity bonuses, promotions, trainings, educational licenses, **criminal record (where required)[69], date of** commencement of employment.

5. Data relating to your health, in so far as they are a prerequisite for the fulfilment of the Company's legal obligations to you under labor law, social security and social protection law and/or other specific laws, such as the granting of sick leave or other special-purpose leave and/or necessary to protect and safeguard the health and safety of workers in the company's working environment.

[66] *Fill in full legal name or first and last name in case of sole proprietorship.*
[67] *Fill in the distinctive title (commercial name) of the company, if any.*
[68] The data mentioned is indicative and each Company should check what is applicable to it.
[69] Each company should request and keep a copy of a criminal record only if specifically required by a legal provision.

6. Your social security data, i.e. notification to Unified Social Security Fund, notice of recruitment to the Manpower Employment Organization (where required), retirements, copies of certificates regarding your compulsory insurance.

7. Bank account (Bank and IBAN) for crediting your fees.

8. Access data of the employee to the Company's computer network and databases, as well as to the internet from fixed and/or portable electronic devices of the Company (e.g. laptops, mobile phones, tablets), and/or data stored in them, in accordance with the Company's policy/regulation for the use of its electronic means.

9. Photos and videos of audiovisual material concerning you, in the context of social events and/or promotional actions of the Company.

10. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

The above personal data under points 1 to 7 are provided to the Company by you and you must update them so that it is complete and accurate during your employment. The provision of your data is your legal obligation and a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide them. The above data concerning your evaluation during your employment in the Company, as well as points 8 to 9 [and 10] arise during your employment in the Company.

C. Purposes and legal basis for processing

The Company collects and processes the aforementioned personal data concerning you for the following purposes and legal bases:

1) Execution of the employment contract

The data under points 1, 2, 4 and 8 of Section B above for identification, communication with you, your professional skills and your development in the Company are processed for the purpose of managing the contractual relationship under the relevant employment contract and the legal basis for processing them is the performance of the contract between the employee and the Company.

2) Keeping a register and individual employee records

The data referred to in points 3, 4, 5 and 6 above of Section B are processed for the purpose of keeping a register and individual records of employees for the fulfilment of the undertaking's obligations arising from the legislation, i.e. labor law and/or social security and social protection law, tax law and the legal basis is the compliance of the Company with a legal obligation.

3) Execution of payroll

The data referred to in points 1, 3, 4 and 5 above of Section B showing the assessment of the wage situation, the productivity bonuses and the data referred to in point 7 of that Section relating to the details of your bank account, are processed for the purpose of carrying out the payroll and fulfilling the undertaking's obligation under the law and the legal basis is the compliance of the Company with a legal obligation.

4) Promotion of the Company in the context of social events and/or promotional actions

The data referred to in point 9 above of Section B relating to audiovisual material shall be processed, provided that you have given your consent, which is the legal basis for processing, for the purpose of promoting the Company in the context of social events and/or promotional activities.

5) Additional benefits to the employee

In order to receive the additional benefits, such as your inclusion in a group insurance program, the data referred to in points 1 and 2 in Section B are processed, provided that you have given your consent, which is the legal basis for processing.
In particular, for your inclusion in a group insurance program of the Company, your data referred to in points 1 and 2 in Section B may be transferred to the insurance company cooperating with the Company, provided you have given your consent, for your voluntary inclusion in the company's group insurance program, for which you then contact the insurance company yourself.

[If paragraph 5 applies, otherwise the Company shall delete it]

6) [insert any other legitimate purposes and their legal basis]

D. Data transfer – Recipients

In order for the Company to fulfil the aforementioned functions and obligations, it communicates your personal data to categories of persons or bodies (recipients). The recipients have access only to those of your personal data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken towards the Company. The categories of recipients are the following:

1. Processors: the Company shall cooperate with the following processors on its behalf in order to assist it in the performance of its legal or contractual obligations, which are
   - accounting service providers: company.....[70],
   - providers of IT support services: company.....,
   - providers of hosting services, cloud providers: company.....,
   - physical security service providers: company.....,
   - [insert any other category of providers]

   subject to the confidentiality of your data.

2. Financial institutions

3. Tax authorities, social security institutions, health bodies (e.g. National Public Health Organization), if provided for by law.

[70] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

4. Lawyers, in so far as this is necessary for the operation of the contract, the performance of the undertaking's statutory or contractual obligations or for the exercise of its rights and the protection of its legitimate interests

5. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as audit/supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

6. Affiliated insurance services companies, for your inclusion in the collective insurance program of the Company. [if applicable, otherwise the Company shall delete it]

7. [insert any other legitimate addressees]

E. Time of data retention

Option A [specify a specific time interval]:

In the context of your contract of employment/cooperation with the Company, your data will be kept for as long as you retain the status of worker in the Company, and after termination for any reason of your employment relationship with the Company for..... [specify period] based on..... [specify the provision of law on the basis of any specific legislation (indicative tax, insurance, labor law)].

Option B [if option A is not possible, please specify the criteria determining the time period for retention]:

In the context of the contract of employment/cooperation concluded with the Company, your data will be kept for as long as you retain the status of worker in the Company, and after termination for any reason of your employment relationship with the Company until..... [specify the criteria determining the period of retention such as the expiry of the limitation period of the claims concerned][71]

If, by the end of the above periods, judicial proceedings are ongoing, in which the Company is involved and directly or indirectly concern you, the time for keeping your data shall be extended until a final judgment is issued.

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the company].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

[If a transfer occurs, then the purposes and addressees must be indicated as follows:]

[71] The maximum period of retention can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

The Company transfers to..... [insert company details and the country in which it is based] to fulfil its purpose..... [insert specific purpose of transfer], with legal basis.....[insert specific legal basis] and if one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, i.e. the establishment, exercise or defense of rights and/or legal claims of the undertaking, or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[The Company is obliged to inform accordingly of any new transfer]

G. What rights do you have in relation to your data and how to exercise them

As employees, you have a number of rights, in accordance with the provisions of Articles 15-22 GDPR, to your personal data processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company]. Or in writing [insert the Company's postal address]. In this case, for the purpose of making the check of your id, you should attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Center (KEP) or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
Performance of the employment contract	Performance of contract (ref. 6.1.b GDPR)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

Keeping a register and individual employee records	Compliance with a legal obligation (Nos 6.1c and 9.2b for special categories)	Access (15) Rectification (16) Restriction (18)
Execution of payroll	Compliance with a legal obligation (No 6.1c)	Access (15) Rectification (16) Restriction (18)
Promotion of the company with photographs and videos in which employees appear (on the website, in brochures, etc.)	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) (Rectification 16) Erasure (17) Restriction (18) Portability (20)
Voluntary benefits to employees such as inclusion in a group insurance program	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

It is noted that the Company has the right in any case to refuse partially or in full your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the performance of the employment contract, as well as for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that your rights mentioned above have been infringed, you have the possibility to lodge a complaint with a supervisory authority. The competent supervisory authority for Greece is the Data Protection Authority, Kifissias 1-3, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[72] of our company, at: Tel.....Email……

H. Confidentiality and confidentiality of the Employee

For its part, the employee is obliged to maintain confidentiality and confidentiality of any personal data of either other employees or other categories of data subjects, such as customers, suppliers, who come to their

[72] If there is a DPO.

knowledge in the performance of their duties. It does not carry out any communication, transfer, storage, retention or other processing of personal data that is outside the tasks assigned to it and is not provided for in the Company's policies and procedures.

5.2.9 Template for the provision of information to prospective employees

INFORMATION TO POTENTIAL EMPLOYEES OF THE COMPANY
.....
ON THE PROCESSING OF PERSONAL DATA

A. Controller's details

Our company with the name[73]..... (and distinctive title[74].....) established in....., No..... tel....., email: ..... (hereinafter referred to as **"Company**") hereby informs you, as controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, the time of their retention, their transfer outside the EU and your rights in relation to your data as customers of the Company and how you can exercise them.

B. Type of data and sources

The personal data collected from you and processed by the Company are[75]:

1. **Identification details, i.e.** full name, father's name and mother's name, ID number, gender, date and place of birth, nationality

2. **Your contact details**, i.e. postal and e-mail address, telephone number (landline, mobile)

3. Curriculum vitae, marital status, any disabilities

4. Training and prior experience, professional experience

5. Ground for refusal of a recruitment application

6. **[add any other data** you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

For the purpose of assessing your application, the Company will collect information about you from your previous employers and from employment and evaluation agencies, provided you have given your consent to them.
[In case the Company does not collect the above information, it should delete the last paragraph.]

The above personal data under points 1 to 4 are provided to the Company by you if you express an interest in the job.

[73] Complete full legal name or first and last name in case of sole proprietorship.
[74] Fill in the distinguishing title (commercial name) of the company, if any.
[75] The data mentioned is indicative and each Controller should check what is applicable to his/her case.

C. Purposes and legal basis for processing

The Company collects and processes your data to the extent that this is required during the interview and possible recruitment process, in order to assess the fulfilment of your recruitment conditions for a specific job in the Company.

The processing of your data is necessary for the legitimate interest we seek in our efforts to recruit qualified and appropriate staff for the purposes of our business.

If you wish to retain your data on possible employment opportunities in our Company in the future and inform you of the possibility of hiring, you should give us your consent for this purpose.

D. Data transfer – Recipients

In order for the Company to fulfil the aforementioned functions and obligations, it communicates your personal data to categories of persons or bodies (recipients). The recipients have access only to those of your personal data that are strictly necessary for the performance of the tasks or the provision of the services they have undertaken towards the Company. The categories of recipients are the following:

1. Processors: the Company cooperates with processors on its behalf to assist it in fulfilling its legal obligations, which are:
   - providers of IT support services: company.....,
   - providers of hosting services, cloud providers: company.....,
   - **[insert any other processors]**

   subject to confidentiality of your data

   [In case the Company does not transmit the data of the prospective employee to the Processors delete point 1 and renumber the following categories]

2. Lawyers, in so far as this is necessary for the fulfilment of the Company's statutory obligations or for the exercise of its rights and the protection of its legitimate interests.

3. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as audit/supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

E. Time of data retention

In case you accept the offer to work in the Company, your personal data will be retained on the basis of the "Information for Workers on the Processing of Personal Data", which is communicated to all Employees.
The personal data of prospective employees who will not enter into a contract of employment with the Company shall be retained for six months after the job for which they were collected.
In case you wish to keep your data on possible job opportunities in the future, please choose the time frame you want:

1 year □ **2 years** □

After the expiry of the above time frames, your personal data will be erased/destroyed [on the basis of the data destruction policy].

F. Transfer of data outside the EU

The Company does not transfer your personal data to third countries outside the EU.

G. What rights do you have in relation to your data and how to exercise them

As prospective employees, you have a number of rights, in accordance with the provisions of Articles 15-22 GDPR, to your personal data processed by the Company.

The table below lists your rights per processing purpose and corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company]. Or in writing [insert the Company's postal address]. In this case, for the purpose of making the check of your id, you should attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Center (KEP) or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS
The assessment of the fulfilment of your recruitment conditions for a specific job	Interest (6.1f)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21)
Inform you about future job opportunities in the Business	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

Please note that the Company has the right in any case to partially or fully refuse to comply with your request to restrict the processing or erasure of your data, if the processing or retention of your personal data is necessary for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply, you consider that the aforementioned rights have been infringed, you can file a complaint to the Personal Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[76] of our company, at: Tel.....Email…….

5.2.10 Template for the provision of information to individuals in case of a personal data breach

INFORMATION ON THE PROCESSING OF PERSONAL DATA OF COMPANY
.....
IN THE EVENT OF PERSONAL DATA BREACH INCIDENT

A. Controller's details

The company bearing the name[77]..... (and distinctive title[78].....) established in ..... (street....., no. … tel..... e-mail: .....), (hereinafter referred to as **"Company**") hereby informs you, as controller, in accordance with Regulation (EU) 2016/679 (hereinafter referred to as "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, the recipients of such data, the time of their retention, their transmission outside the EU and your rights in relation to your data and how you can exercise them in the event of an incident of a personal data breach; it is necessary to process your data in order to fulfil the Company's obligations under Articles 33 and 34 of the GDPR.

General information: The GDPR, in Articles 33 and 34, requires controllers to deal with any incident of a personal data breach. In particular, three cases can be distinguished:
A) The incident may pose a risk to the rights and freedoms of the data subjects concerned.
The controller must report the incident to the Personal Data Protection Authority.
B) The incident may pose a high risk to the rights and freedoms of the persons concerned.
The controller shall:
a) report the incident to the Authority; and
b) communicate the incident to the data subjects concerned in plain and comprehensible language.
C) In any case, whether or not the incident causes/incurs a risk to the rights and freedoms of affected data subjects concerned, *the controller shall record the incident in a specific internal register ("data breach record")*
The notification to the Authority shall be made without delay and no later than 72 hours after the controller becomes aware of the incident.
The notification must contain specific information (e.g. nature/extent of the incident, categories of persons affected, cause and consequences thereof, actions taken to deal with it, etc.). Even if not all of this information is available at the time of submission of the notification, it should be submitted as an initial notification and then updated without undue delay (submitting an additional notification).
Communication to natural persons should be made without delay, i.e. in less than 72 hours, in the most appropriate and effective manner, in the form of personalized information and not through a general communication, to the extent possible.

[76] *If there is a DPO.*
[77] Complete full legal name or name in case of sole proprietorship.
[78] Fill in the distinctive title (trade name) of the company, if any.

B. Type of data and sources of origin

When notifying the Data Protection Authority of a data breach incident, no personal data shall in principle be processed. Only the ***incident*** (description) including information on which categories of ***data*** have been breached shall be disclosed.

Only, if there is an obligation to notify the subjects, the Company processes your data in its records consisting of contact information such as *telephone or email or (social media)*. For the reason that the notification must be made **immediately** *(*without delay) it is not recommended to use a *postal address* unless the above information is not available. In particular, if the above information is not available or it has been breached, as a result of which it no longer exists in the company's records, it will make a *public announcement by electronic or printed press*.

C. Purpose and legal basis for processing

The Company collects and processes the above mentioned personal data concerning you for the purpose of complying with a legal obligation to investigate the occurrence of a data breach, communicate it to you if you are affected by it, and record the incident in its internal register/record.

If you are affected by the incident of breach, you will be informed by any means involving **direct** communication (e.g. E-mail or other contact details). In the event of lack of contact details or if the number of persons affected is particularly large, so that your immediate individual information becomes impracticable, the Company may inform you, as affected person (data subjects) through the press. The legal basis for this is the fulfilment of the Company's legal obligations under Articles 33 and 34 GDPR.

D. Transfer of data – Recipients

The Company only communicates to you those data that are strictly necessary:

1. To the processor-company..... with which it contracted for the investigation of the incident of breach.
2. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

E. Data retention time

Option A [specify a specific time interval]:

The Company keeps your data to document the breach incident in the relevant record *("data breach record"),* in order to fulfil its obligation under Article 33(5) GDPR, within the accountability principle, for [specify period of time].

Option B [if option A is not possible, please specify the criteria determining the time period for retention]:

Your data to substantiate the breach event is kept in the relevant record *("data breach record"),* in order to fulfil the obligation of the Company pursuant to Article 33(5) GDPR, within the accountability principle, until [specify the criteria that determine the period of retention such as the expiry of the limitation period of the claims concerned] [79]

After the expiry of the above time intervals, your personal data will be erased/destroyed [on the basis of the destruction policy of the company].

[The GDPR does not specify any period of time to keep the documentation of the breach event ("data breach record"). Where such a record contains personal data, it will be for the controller to determine the appropriate retention period, in accordance with the principles relating to the processing of personal data and to carry out the processing on a lawful basis. It should keep the above record, in accordance with Article 33(5) GDPR, as proof of compliance with this Article in the context of the accountability principle. It goes without saying that, if the above record does not contain personal data, the principle of limiting the storage period of the GDPR does not apply and therefore there is no question of an obligation on the controller to set a specific retention period on the basis of that principle.]

F. Transfer of data outside the EU

Your data is not transferred outside the EU for the above purpose.

G. What rights do you have in relation to your data and how to exercise them

If your personal data has been violated, you have a number of rights, in accordance with the provisions of Articles 15-22 GDPR, to your personal data processed by the Company.

The table below lists your rights based on the purpose of the processing and a corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

If you wish to exercise a right, please fill in the corresponding form and send it to the email address [insert e-mail of the Company] or in writing [insert the Company's postal address]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizen's Service Centre (KEP) or a police authority.

PURPOSE	LEGAL BASIS	RIGHTS

[79] The maximum period of retention can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

Investigating the incident of breach and informing subjects affected by the incident and recording the incident in the relevant internal register/record of the company ('data breach documentation record')	Compliance with legal obligation (6.1c + 33, 34 GDPR)	Access (Article 15 GDPR) Rectification (16) Restriction (18)

The Company must reply to your request within one month of receipt. This time limit may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform you within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on your request in the exercise of the above rights or following its reply you consider that the above mentioned rights have been infringed, you have the possibility to lodge a complaint with the Data Protection Authority, 1-3 Kifissias Avenue, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

For any matter relating to the protection of your personal data, please contact the Data Protection Officer[80] of our company, at: Tel.....Email…….

5.2.11 Template for the provision of information on video surveillance

Information to the controller on the obligation to inform data subjects for the processing of personal data through a video surveillance system

Any person (natural or legal person) who intends to install a video-surveillance system **for the purpose of protecting persons and property** in an area which it manages, becomes the controller of that processing and must ensure that it is lawfully carried out.

The controller must display an appropriate number of visible information signs regarding video surveillance. In any event, it must provide the persons concerned with the processing with full information on it, so as to ensure that such processing is fair and transparent. In particular, it should provide all the information described in Article 13 of the General Regulation (EU) 2016/679 (hereinafter GDPR). Basic information on the processing can be provided through the information signs, while additional information must be available in another way (e.g. a form or a website), at a second level of information.

Templates for informing data subjects

A. First-level information

At the first level, warning signs are required, indicating the basic characteristics of the processing. The signs shall be so placed as to be clearly visible from all possible points of entry to the surveillance area.

[80] *If there is a DPO.*

Mandatory first level information:

- Purpose of the processing
- Identity of the controller and/or its representative
- Reference to the rights of the data subject
- Reference to the detailed information (2nd level of information). It is recommended to use a link to a website (with URL or QR). If the controller does not have a website, he/she must refer to the location where the data subjects can find the detailed information.
- Indication of the contact details of the Data Protection Officer (DPO) in case one has been appointed.

Furthermore, in the event that the processing is not included as typically expected by a data subject, the first level sign should include further information, such as transfers to unexpected third parties (e.g. non-EU transfer) or exceeding the data retention periods set out in the Authority's Directive 1/2011. Article 9 of Directive 1/2011 identifies the expected recipients, such as the competent law enforcement authorities.

Model **first-level** information signs:

Using QR code:

i. **and DPO data reference (doc — pdf)**

ii. No DPO data reference (doc — pdf)

Without QR code:

i. **and DPO data reference (doc — pdf)**

ii. **No DPO data reference (doc — pdf)**

B. Second-level information

The information in the second level must be posted in an easily accessible space for the data subjects. Posting them on a website is a good practice, but must also be accompanied by non-electronic information, for those who do not have direct electronic access. At this level, detailed information on all the features of the processing is required, as provided for in Article 13 of the GDPR. It should be pointed out that, in its Directive 1/2011, the Authority had, already in 2011, provided for multi-level information. Now, with the application of the GDPR, the augmented second level information is required without the subject's request.

In particular, in addition to the first level information, which must be presented in more detail, typical video surveillance systems require the following to be included in the information:

- The full identity and contact details of the controller and, where available, of the controller's representative.

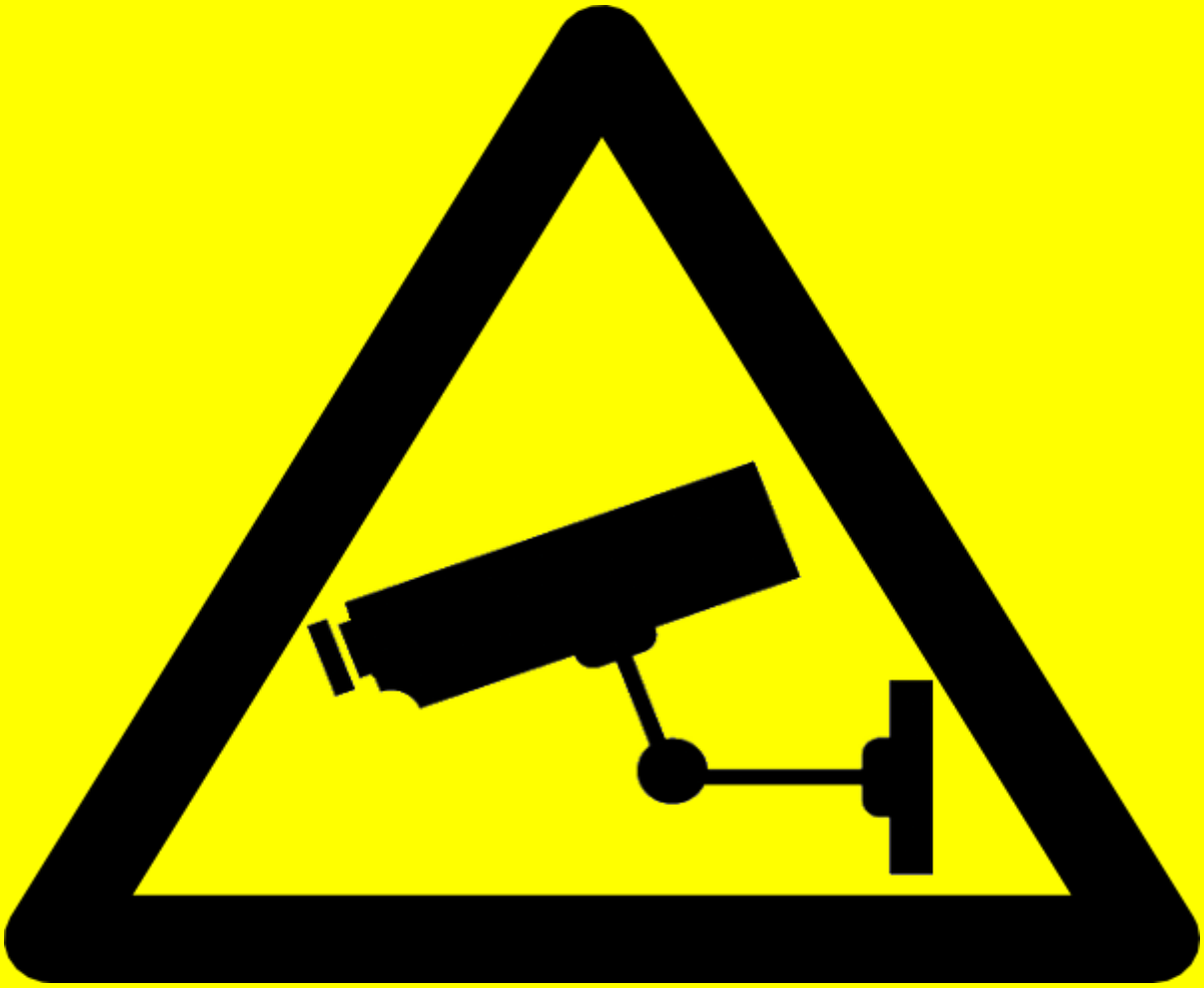
- Contact details of the Data Protection Officer, if designated.
- The purpose of the processing and the legal basis for the processing. In cases where processing differs from formal, detailed specification of the purpose of the processing is required. Typical processing activities are in particular those identified in the Authority's Directive 1/2011.
- The legitimate interests pursued by the controller when processing is based on Article 6(1)(f) GDPR, as is the case in most cases.
- The types of data and the categories of data subjects.
- The recipients or categories of recipients of the personal data (see also Article 9 of Directive 1/2011). This includes the categories/qualifications of persons operating the system.
- Information on the transfer of data to a non-EU country, if this is the case.
- The period of time for which the data are stored.
- How the data subject can exercise his or her rights under personal data protection law, specifying which rights apply. Please note that in typical video surveillance systems the rights of access, restriction, opposition and deletion apply, while other rights may be applied in exceptional cases.
- Information on the right to lodge a complaint with a supervisory authority and the details of the supervisory authority.

Example of second level information text:

For a typical small and medium-sized business with a shop serving customers is available in section 5.2.13.

5.2.12 Templates for the provision of first level (A-level) information on video surveillance

5.2.12.1 First level (A-level) information withoutQR_withoutDPO



THERE IS A VIDEO SURVEILLANCE SYSTEM IN PLACE FOR THE PROTECTION OF PERSONS AND GOODS

For more detailed information and for the exercise of rights under Regulation (EU) 2016/679 (GDPR), please refer to:

Controller according to GDPR:

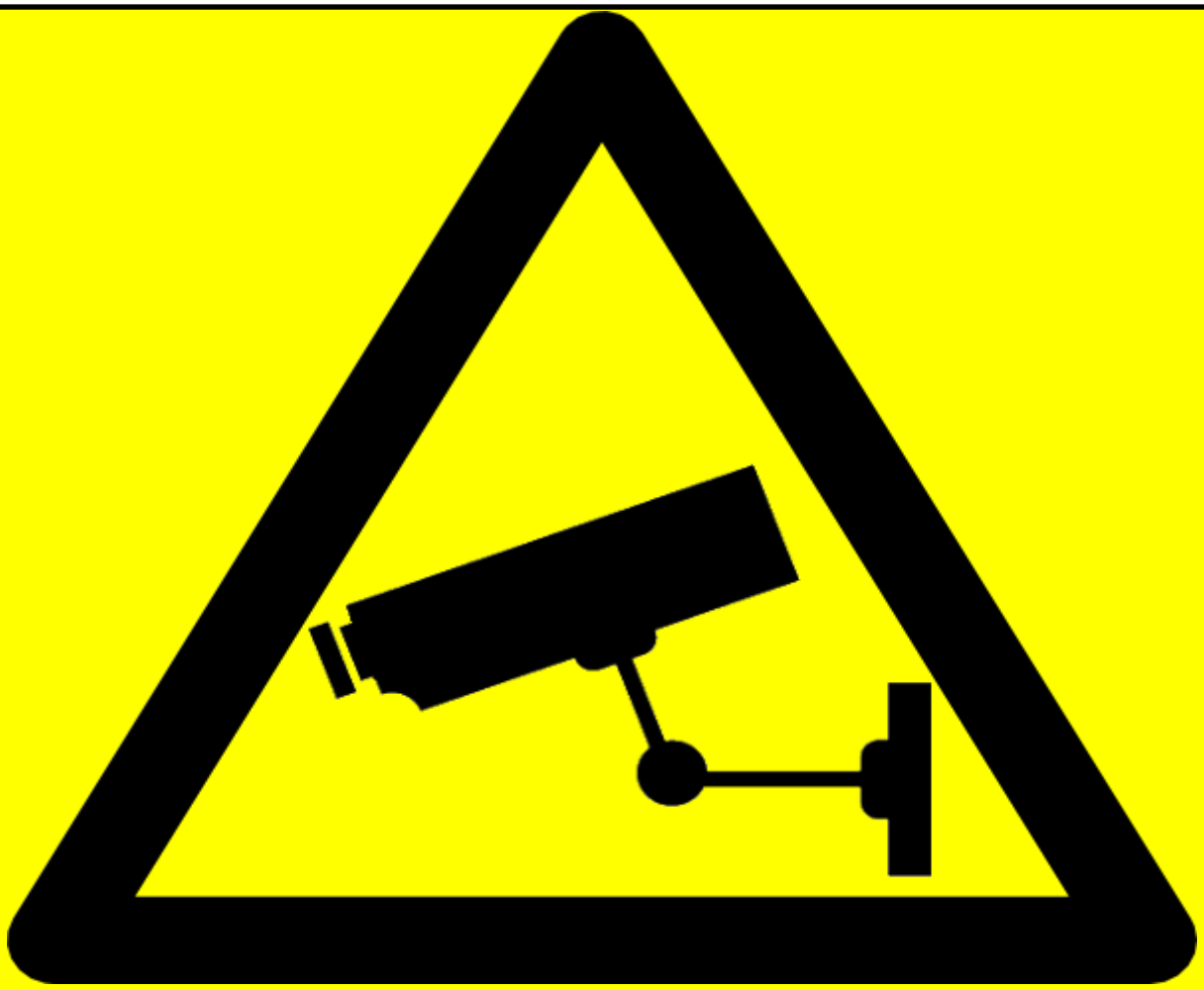
Instructions for use:

Purpose of processing: Modify appropriately in case of purpose differentiation.

More detailed information and exercise of rights: Please indicate where in the store/building the data subjects can find the detailed level B information. The reference may be made to a website.

Controller: Enter the contact details of the controller. In case the controller is established outside the EU, you should include the details of his/her representative, according to Article 27 GDPR.

5.2.12.2 First level (A-level) information withoutQR_withDPO



THERE IS A VIDEO SURVEILLANCE SYSTEM IN PLACE FOR THE PROTECTION OF PERSONS AND GOODS

For more detailed information and for the exercise of rights under Regulation (EU) 2016/679 (GDPR), please refer to:

Controller according to GDPR:

Contact details of Data Protection Officer (DPO):

Instructions for use:

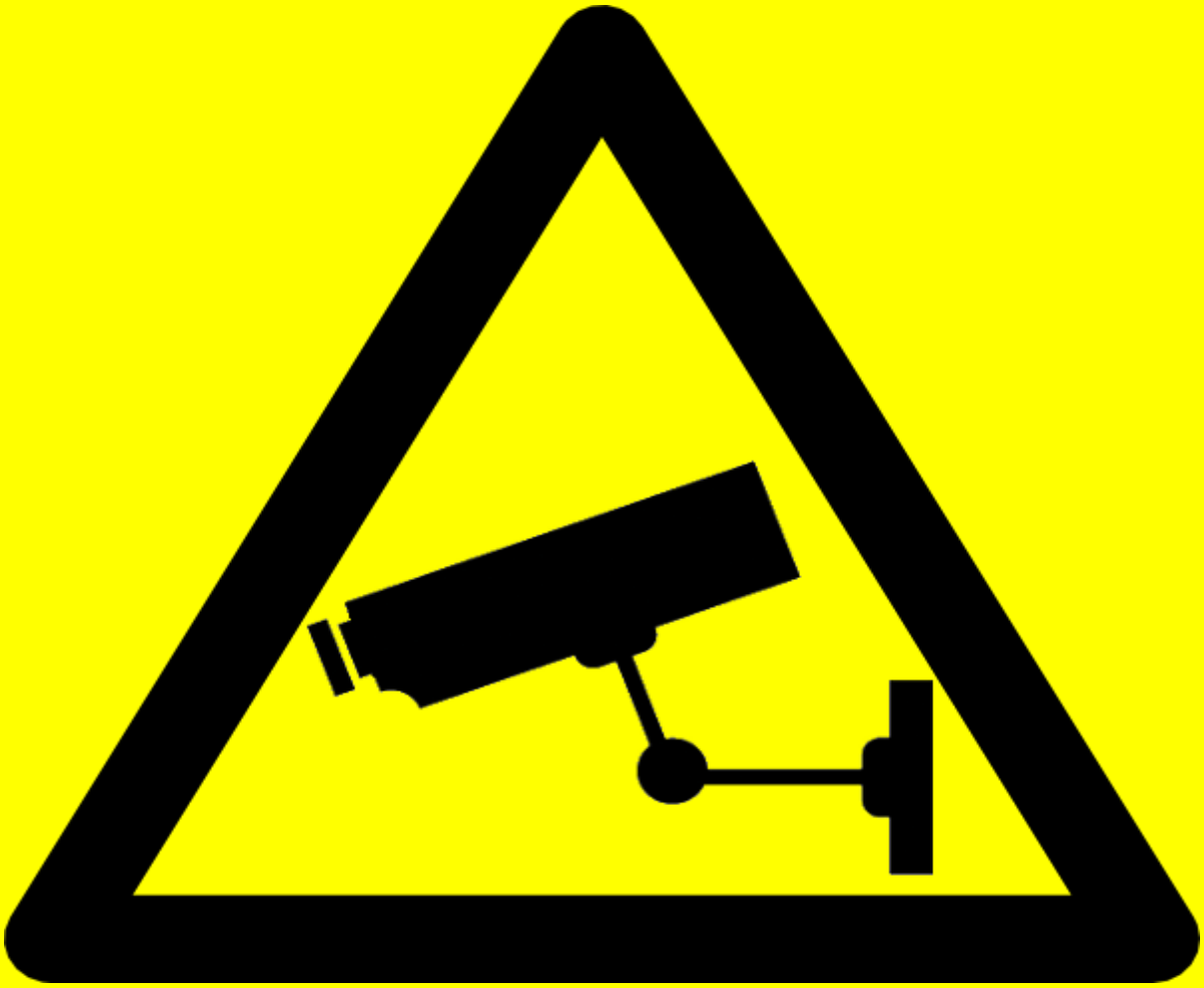
Purpose of processing: Modify appropriately in case of purpose differentiation.

More detailed information and exercise of rights: Please indicate where in the store/building the data subjects can find the detailed level B information. The reference may be made to a website.

Controller: Enter the contact details of the controller. In case the controller is established outside the EU, you should include the details of his/her representative, according to Article 27 GDPR.

Data Protection Officer: Enter the contact details of the Data Protection Officer so that the data subject can contact him/her on issues related to the processing of his/her data.

5.2.12.3 First level (A-level) information withQR_withoutDPO



THERE IS A VIDEO SURVEILLANCE SYSTEM IN PLACE FOR THE PROTECTION OF PERSONS AND GOODS

For more detailed information and for the exercise of rights under Regulation (EU) 2016/679 (GDPR), please refer to:

Controller according to GDPR:

Instructions for use:

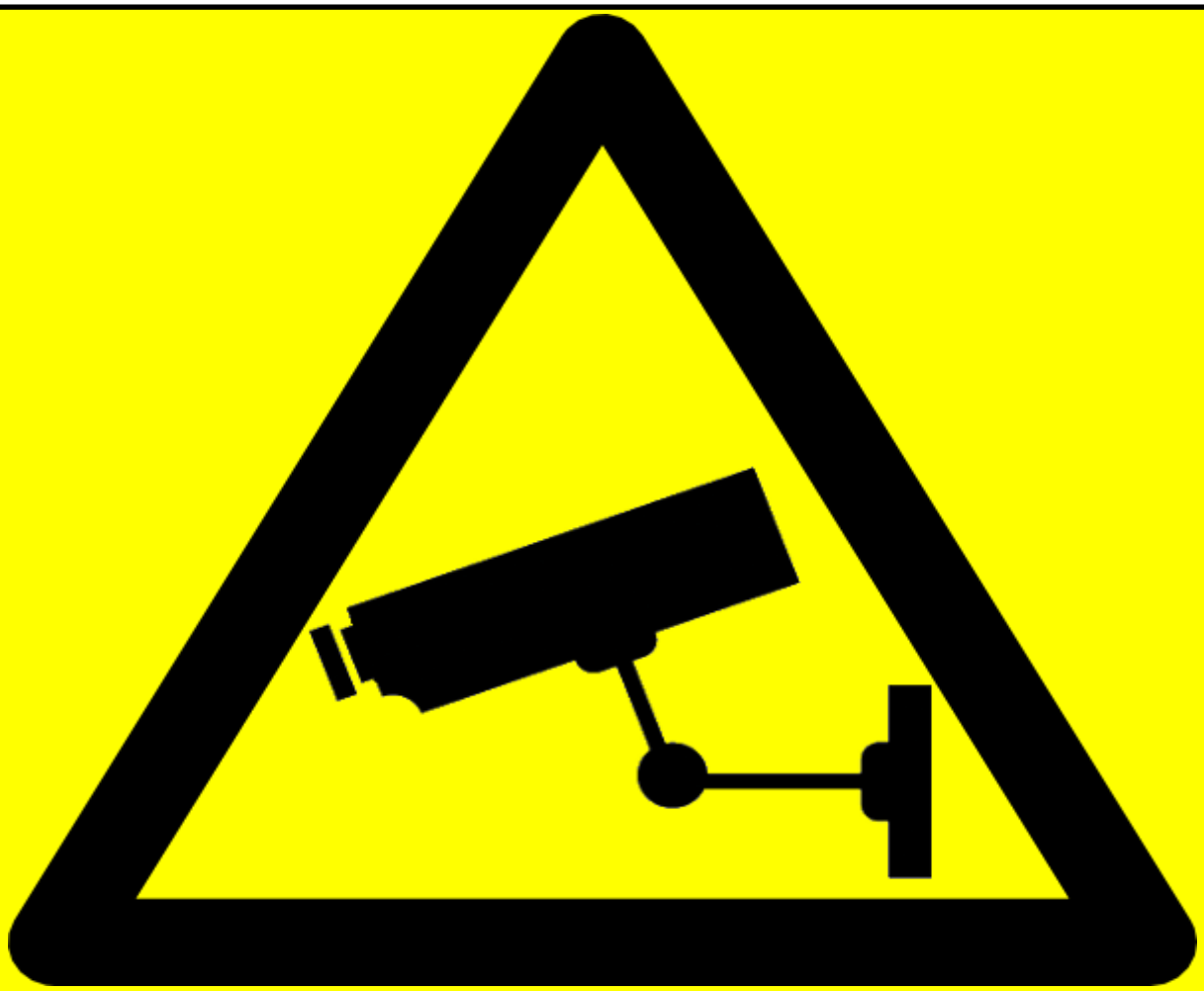
Purpose of processing: Modify appropriately in case of purpose differentiation.

More detailed information and exercise of rights: Please indicate where in the store/building the data subjects can find the detailed level B information. The reference may be made to a website.

QR code: If you refer to a website, modify the image by inserting a link to the website with the second level information.

Controller: Enter the contact details of the controller. In case the controller is established outside the EU, you should include the details of his/her representative, according to Article 27 GDPR.

5.2.12.4 First level (A-level) information withQR_withDPO



THERE IS A VIDEO SURVEILLANCE SYSTEM IN PLACE FOR THE PROTECTION OF PERSONS AND GOODS

For more detailed information and for the exercise of rights under Regulation (EU) 2016/679 (GDPR), please refer to:

Controller according to GDPR:

Contact details of Data Protection Officer (DPO):

Instructions for use:

Purpose of processing: Modify appropriately in case of purpose differentiation.

More detailed information and exercise of rights: Please indicate where in the store/building the data subjects can find the detailed level B information. The reference may be made to a website.

QR code: If you refer to a website, modify the image by inserting a link to the website with the second level information.

Controller: Enter the contact details of the controller. In case the controller is established outside the EU, you should include the details of his/her representative, according to Article 27 GDPR.

Data Protection Officer: Enter the contact details of the Data Protection Officer so that the data subject can contact him/her on issues related to the processing of his/her data.

5.2.13 Template for the provision of second level (B-level) information on video surveillance

Information on the processing of personal data through a video surveillance system of the Company

……

1. **Controller' details:**

The Company bearing the name[81]…… (and distinctive title[82]……) established in…… (street……, no. …. tel…… e-mail: ……), (hereinafter referred to as **"Company**") hereby informs you, as the controller, in accordance with Regulation (EU) 2016/679 (hereinafter "GDPR") and the relevant provisions of Greek legislation on the protection of personal data, as applicable, on the type of personal data collected, the source of their collection, the reason for their collection and processing, any recipients thereof, the time of their retention, their possible transfer outside the EU and your rights in relation to your data and how you can exercise them.

2. **Purpose of processing and legal basis:**

We use a surveillance system for the purpose of protecting persons and property. Processing is necessary for the purposes of legitimate interests we pursue as a controller (Article 6(1) in the General Regulation (EU) 2016/679, hereinafter referred to as GDPR).

Our legitimate interest is the need to protect our premises and property from illegal acts, such as theft. The same applies to the safety of life, physical integrity, health and property of our staff and third parties legally present in the supervised area. We limit reception in places we assessed that there is an

81 Complete full legal name or name in case of sole proprietorship.

82 Fill in the distinctive title (trade name) of the company, if any.

increased likelihood of unlawful acts e.g. theft, such as in our cashiers and entrances, without focusing on places where the privacy of the persons monitored may be excessively restricted, including their right to respect for personal data.

3. **Data type and categories of data subjects**

We collect only image data of our employees and third parties, customers and visitors who are legally present in the supervised area.

4. **Recipients**

The material held is accessible only to our responsible/authorized personnel in charge of the safety of the site. Such material shall not be transferred to third parties, except in the following cases: a) to the competent judicial, prosecutor and police authorities when it contains information necessary for the investigation of a criminal offence concerning persons or property of the controller; (b) to the competent judicial, prosecutor and police authorities when requesting data lawfully in the course of their duties; and (c) to the victim or perpetrator of a criminal offence, in the case of data which may constitute evidence of the offence.

5. **Data retention time**

We keep the data for seven (7) days, after which they are automatically deleted. If during this time we find an incident, we isolate part of the video and keep it up to one (1) month, with a view to investigating the incident and initiating legal proceedings to defend our legitimate interests, while if the incident concerns a third party we will keep the video for up to three (3) months.

6. **Rights of data subjects**

Data subjects shall have the following rights:

- Right of access: you have the right to know if we are processing your image and, if so, to obtain a copy of it.
- Right to restriction: you have the right to ask us to restrict the processing, for example not to delete data that you consider necessary to establish, exercise or support legal claims.
- Right to object: you have the right to object to processing.
- Right to erasure: you have the right to request that we delete your data.

You can exercise your rights by sending an e-mail to privacy@ypodeigma.gr or letter to our postal address or by submitting the request in person to our company's address [insert your address]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre (KEP) or a police authority.

The table below lists your rights based on the purpose of the processing and a corresponding legal basis. In this table you will find detailed information (concept, method and time limits) and form for the exercise of each right. General information on the exercise of your rights is available here.

PURPOSE	LEGAL BASIS	RIGHTS
Video surveillance for the protection of persons and goods	Overriding legitimate interest (6.1f)	Access (15) Erasure (17) Restriction (18) Objection (21)

In order to consider a request related to your image, you will need to determine when you were about in the range of the cameras and give us a picture of you, so as to make it easier for us to locate your own data and hide the data of third-party persons. Alternatively, we give you the opportunity to come to our premises to show you the images in which you appear. We also note that the exercise of the right to object or erasure does not entail the immediate deletion of data or modification of the processing. In any case we will reply in detail as soon as possible within the deadlines set by the GDPR.

7. **Right to file a complaint**

In case you consider that the processing of your data is in breach of the GDPR, you have the right to file a complaint with a supervisory authority.

The competent supervisory authority for Greece is the Data Protection Authority, Kifissias 1-3, 115 23, Athens, https://www.dpa.gr/ tel. 2106475600.

5.2.14 Table matching processing purposes with legal bases and data subjects' rights

OVERALL TABLE FOR THE MATCHING OF PROCESSING PURPOSES WITH LEGAL BASES AND RIGHTS OF THE COMPANY **……**			
PROCESSING ACTIVITIES	**PURPOSE**	**LEGAL BASIS**	**RIGHTS**
A. Customer management **(Health sector)**	Provision of health services (identification and communication details)	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

	Provision of health services (health data)	Contract with a health professional bound by secrecy (9.2h)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Invoicing of services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
	Promotion of services to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)
A. Customer Management (Tourism-Hospitality sector)	Provision of hotel and tourism services (identification and communication details)	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Provision of hotel and tourist services (with regard to any health data, e.g. food and accommodation preferences)	Consent (9.2a)	Withdrawal of consent (7.3) Access (15) Rectification(16) Erasure (17) Restriction (18) Portability (20)
	Invoicing of products/services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
	Promotion of products/services to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)

A. Customer Management (Education sector)	Provision of training services to customers (identification and communication details)	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Provision of training services to customers (study/performance data)	Compliance with a legal obligation (6.1c) based on a specific provision of educational legislation as appropriate	Access (15) Rectification (16) Restriction (18)
	Keeping of an individual student health card	Compliance with a legal obligation in the field of social protection (9.2b)	Access (15) Rectification (16) Restriction (18)
	Invoicing of services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
	Photoshooting of students/videos of events	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Promotion of services to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)
A. Customer Management (Commerce sector)	Supply of retail trade services of products including distance e-shop services (identification and communication data)	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Invoicing of products	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)

	Promotion of products to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)
	Optional participation in a customer loyalty program (loyalty/bonus)	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
A. Customer management **(Other sector)**	Provision of products or services to customers in general (identification and communication details)	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Invoicing of products/services	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)
	Promotion of products/services to customers by electronic means	Overriding legitimate interest (6.1f + Law 3471/2006 11.3)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21) Objection and human intervention in automated decision (22)
	Optional participation in a customer loyalty program (loyalty/bonus)	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
B. Personnel management	Performance of the employment contract	Performance of contract (6.1.b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

	Keeping a register and individual employee records	Compliance with legal obligation (6.1c and 9.2b for special categories) + labour legislation	Access (15) Rectification (16) Restriction (18)
	Execution of payroll	Compliance with legal obligation (6.1c) + labour law	Access (15) Rectification (16) Restriction (18)
	Promotion of the company with photographs and videos depicting employees (on the website, in brochures, etc.)	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Optional employee benefits such as inclusion in a group insurance policy	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
C. Management of potential employees	The assessment of the fulfilment of your recruitment conditions for a specific job	Legitimate interest (6.1f)	Access (15) Rectification (16) Erasure (17) Restriction (18) Opposition (21)
	Information about future job opportunities in the Company	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
D. Management of suppliers (natural persons)	Supply of products/services to the Company	Performance of a contract (6.1b)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
	Fulfilment of tax obligations	Compliance with legal obligation (6.1c) + tax legislation	Access (15) Rectification (16) Restriction (18)

E. Video surveillance	Video surveillance for the protection of persons and goods	Overriding interest (6.1f)	Access (15) Erasure (17) Restriction (18) Objection (21)
F. Outreach of potential customers	Promotion of products/services to potential customers by electronic means	Consent (6.1a + Law 3471/2006 Art. 11.1)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
G. Personal Data Breach Management	Investigation of the incident of breach and informing subjects affected by the incident and recording the incident in the relevant internal register/record of the company ('data breach record')	Compliance with legal obligation (6.1c + 33, 34 GDPR)	Access (15) Rectification (16) Restriction (18)

5.3 Consent

5.3.1 Frequently Asked Questions about consent as a legal basis for personal data processing

1. What is the meaning of consent?

Consent means any indication of intention, freely given, specific, informed and unambiguous, by which the data subject expresses his/her agreement, by a statement or by a clear affirmative action, to the processing of personal data relating to him or her.

2. Is consent necessary for the processing of data?

No, it's not necessary. Personal data may be processed lawfully using other legal bases, such as performance of a contract, compliance with a legal obligation of the controller and processing to fulfil the overriding legitimate interests of the controller or a third party. Indeed, where there is another more appropriate legal basis for data processing, consent should be avoided.

3. What other legal bases for processing exist?

The legal bases for the processing of personal data are six:

a) consent;

b) performance of a contract to which the data subject is a party or in order to take measures at the request of the data subject prior to the conclusion of a contract;

c) processing is necessary to comply with a legal obligation of the controller;

d) processing is necessary to safeguard the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless those interests do not prevail over the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

4. In what cases is the use of consent excluded?

Consent is excluded where there is no real and effective freedom of choice of the subject. This is mainly the processing of employees' data in the context of an employment relationship, or cases where the processing of personal data is necessary for the performance of a contract e.g. room reservation/provision of tourist services in a hotel, provision of health services, provision of education/care services.

5. When is consent the most appropriate legal basis?

Where the data subject is given control and a genuine choice of accepting or rejecting the terms and conditions offered without prejudice. Similarly, where there is a possibility to withdraw consent without the data subject having been harmed or losing substantial benefits.

Consent embedded in a part of the text "terms and conditions" without a separate possibility of negotiation is not valid.

Cases where consent is appropriate are in particular advertising by electronic means e.g. sending e-mails or newsletters, the use of cookies, additional optional employee benefits (such as participation in a private insurance scheme), etc.

6. How should consent be given?

Consent must be given freely and necessarily requires prior information.

This information shall include information on:

- The identity of the controller
- The purpose of each processing operation for which consent is sought
- The type of data collected and used
- The possibility of withdrawing consent for the future
- Any use of the data for automated decisions or profiling
- In the case of transfer outside the EU, information on possible risks.

Information must also be clear and simple — suitable for children when addressed to minors and meet the same conditions as information under the principle of transparency.

Consent must be specific, that is to say, for one or more processing purposes, which must be clearly identified in order to allow a different consent to be given for each different purpose.

Consent must also be explicit. A statement or a clear positive action of the data subject (e.g. selection in a 'box') is required through deliberate action.

On the contrary, tacit acceptance after being informed, but without any action, is not understood as consent. Pre-checked boxes and opt-out boxes are not a valid method of obtaining consent.

Consent may be obtained by any means, provided that the controller can prove that it has been obtained from the data subject. Ideally, it should be a written statement and not an oral statement. In particular, online services may be provided by filling in an electronic form, sent by e-mail, filling in a box when visiting an internet site, selecting the desired technical arrangements for information society services, or using an electronic signature. Consent can also be given by telephone conversation, provided that appropriate information is provided and specific confirmation is requested from the data subject (e.g. by pressing a button or providing an oral confirmation).

Therefore silence, pre-filled boxes or inaction should not be understood as consent.

7. Is consent sufficient for multiple processing purposes?

Consent should cover all processing activities carried out for the same purpose or for the same purposes. Where the processing has multiple purposes, consent should be given per processing purpose rather than consent for all purposes.

8. Is consent limited in time?

The GDPR does not set a specific time limit for the duration of consent. Its duration depends on the scope of the initial consent and the expectations of the data subject. If processing operations change substantially, the initial consent is no longer valid and new consent should be obtained. A good and safe practice is to renew consent at appropriate intervals.

9. I have a business/website that targets/has products and/or services for children. On what terms may their consent be obtained?

Consent as a legal basis for the processing of children's data is used in connection with the offer of information society services (services and goods available online), which are offered directly to a child, only if the child is at least 15 years old, as provided for in Law 4624/2019 and is applicable to Greece. If the child is under 15 years of age, consent from the person with parental responsibility is required.

As age is a critical factor in obtaining consent directly, reasonable efforts must be made to verify that the user is indeed an older person than required for the digital consent.

Where the age of the user, as stated by him/her, is lower than that provided for digital consent, the controller may accept this statement without further checks, but should obtain parental authorisation and verify that the person giving consent is the person who has parental responsibility for the child. The verification in each case depends on the nature and risks of the processing activities.

However, age verification should not lead to the processing of an excessive amount of data.

Verification methods include requiring the user to indicate his/her year of birth or to fill in a form stating that he/she is (not) a minor. The email address of the legal representative of the minor can also be searched to send an email and confirm the consent. The use of a token bank card or a symbolic banking transaction could also be requested cumulatively with the declaration of consent from the child's legal representative.

10. For the processing of personal data of employees in my business, do I have to obtain their consent?

The consent of employees as data subjects in the context of employment relationships cannot be regarded as free due to the inherent inequality of the parties. Due to the dependency relationship that the employer/employee relationship necessarily entails, it is unlikely that the data subject will be able to refuse to give his/her employer consent to the processing of his/her data without fear or without real risk of being adversely affected by his/her refusal.

In such cases another legal basis for processing should be chosen, such as the performance of the employment contract.

However, there may be circumstances in which the employer can prove that consent is in fact freely given, where failure to give consent will have no negative effect on the employee. Such cases include, for example, the processing of employees' personal data in the context of voluntary participation in a private security/health care programme, organisation and participation in a social event or excursion, participation in filming/photoshooting of the workplace.

11. How should the possibility of withdrawing consent be implemented?

As the withdrawal of consent is considered a necessary aspect of valid consent in the GDPR, it must be ensured that the data subject can withdraw his/her consent with the same ease as he/she gave it at any time. Withdrawing it should be as easy as providing it. Where, for example, consent is obtained by electronic means, with a simple mouse click, a button shift or the press of a button, data subjects must, in practice, be able to withdraw such consent as easily as possible in the same way.

12. I process personal data in the course of my business on the basis of consent obtained from data subjects before the GDPR became applicable. Is it still valid?

Consent obtained before the Regulation applies, if it fulfils the conditions, set by the GDPR for the valid obtaining of consent. In essence, the controller must review the procedure by which consent was obtained, the information provided in order to obtain it, the possibility of revoking it proportionately and without hindrance and the manner in which the above is documented.

In case the above-mentioned conditions are not covered, consent should be sought again on the basis of the GDPR. If consent can still not be obtained in accordance with the provisions of the GDPR and after checking the applicability of other legal bases it is found that there is no such possibility, the controller must stop processing personal data.

5.3.2 Template of a customer's declaration of consent

MODEL DECLARATION OF CONSENT

Private School Events - Photography and Video Recording

Our school (name..... title..... having its seat at ..... street..... no. ..... tel..... e-mail: .....), as part of the photography and video recording of the event, organises on ..... (*insert date)*, ... (*insert event name*) will collect and process the image and, where appropriate, the voice of the pupils, parents and guardians attending, as Controller in accordance with Regulation (EU) 679/2016 (General Data Protection Regulation), subject to their consent, in accordance with the conditions described below.

The purpose of the processing (photography and/or video recording) of your face (and/or voice) data is:

- publishing the material on the Internet, on the School's website (www.....) and on the pages of the School Social Media (facebook, Instagram, ... *[complete what is applicable]*) as well as in the daily or periodic press, for the purpose of promoting the services provided.
- sharing the relevant audio-visual material on CD/DVD to students for commemorative purposes;
- keeping the audio-visual material in the school's archives for historical reasons.

The legal basis for the processing of your image data is your consent (which in the case of minor pupils is provided by their legal representatives) in accordance with Article 6(1)(a) GDPR. You are not obliged to give your consent to the collection and processing of your data in the above ways. If you refuse to give your consent, you will be asked to sit at a point where no image is taken or, if this is not possible, the material concerned will be processed to cover your characteristics in a way that makes your image unrecognizable (blurred).

If you give your consent, your data will be retained for as long as we have your consent and until it is revoked. You have the right to withdraw your consent at any time for the future, without affecting the processing that will take place up to the time of withdrawal. In this case we will take all necessary steps to stop the future processing of your image data. In addition, you have the right to access your personal data held by the School, to delete them under the conditions of Article 17 GDPR, to restrict processing under the conditions of Article 18 GDPR, to portability (Article 20 GDPR) and to object to processing (Article 21(1) GDPR), as well as to lodge a complaint with the competent Data Protection Authority (www.dpa.gr).

You can exercise your rights by means of a document to be delivered or sent to the School at the following address ..... or electronically by e-mail to.....@..... . When exercising your rights, you may be asked for documents to identify you.

Having been informed of the above, the undersigned ..... parent/guardian of pupil *[this is filled in only if the undersigned acts on behalf of the minor]* agree to the processing of my/his/her personal data in the following ways:

A. Publishing audiovisual material on the internet for promotional and marketing purposes, in particular

- on the School website (www.....) YES☐ NO ☐__
- on the pages of the School Social Media YES☐ NO ☐__
- in the daily or periodic press YES☐ NO ☐__

B. Sharing relevant audiovisual material on CD/DVD to students for commemorative reasons

YES☐ NO ☐__

C. Keeping audio-visual material in school archives for historical reasons

YES☐ NO ☐__

Full name.....

Address.....

Date.....

Signature/electronic signature

5.3.3 Template of an employee's declaration of consent – collection of material from social event and/or promotional activities

MODEL DECLARATION FOR EMPLOYEE'S CONSENT

For Collection of Material from Social Events and/or Promotional Actions of the Company

Our Company with the name.....and title ..... having its seat in (street..... no. .....

tel..... e-mail: .....) collects and processes personal data of its employees, as Controller in accordance with Regulation (EU) 679/2016 (General Data Protection Regulation).

Personal data are collected for the purpose of promoting the Company with photographs and videos featuring its employees (on the website, in brochures, etc.)

The personal data collected are photographs and audio-visual material [if any of the above mentioned data is not collected, the company may delete it] from your participation in social events and/or events as part of the Company's promotional activities and are retained by the Company for a period of time... [insert the period]. This data is accessible to the processor-partner company providing photography and video recording services. Your data shall remain confidential.

You reserve the right to withdraw your consent by making a request in the ways set out below.

Having taken note of the "Information of employees of the Company on the processing of personal data", as well as the above, I agree to the processing of my personal data for the stated purpose.

Full name.....

Address.....

Date.....

Signature/electronic signature

You may submit this by sending it to the e-mail address of the Company..... [insert e-mail of the Company] using your individual corporate e-mail or in writing..... [insert the postal address of the Company]. In this case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre (KEP) or a police authority.

5.3.4 Template of an employee's declaration of consent – optional benefits

MODEL DECLARATION FOR EMPLOYEE'S CONSENT

For Optional Employee Benefits

Our Company with the name.....and title .....having its seat at (street.....no. .... tel..... e-mail: .....) collects and processes personal data of its employees, as Controller in accordance with Regulation (EU) 679/2016 (General Data Protection Regulation).

Personal data processed for the purpose of offering voluntary, optional benefits by the Company to its employees..... [complete the benefits, e.g. inclusion in a collective life-health insurance policy, the use of a car, meal vouchers] are (a) your identification details, i.e. name, father's name and mother's

name, ID number, tax identification number and tax office number, social security number, gender, nationality, date and place of birth and (b) your contact details, postal address and e-mail address, telephone number (landline, mobile) [insert or delete as appropriate the data processed]

These data shall be kept for the period of time the employee's file is kept by the Company, in accordance with the information provided in the information form.

The Company shall communicate the above mentioned data to the processor-partner service provider..... [insert type of benefit and name of the processor]. Your data shall remain confidential.

[In case this concerns inclusion in a group insurance policy, the previous paragraph should be deleted and the following should be maintained:]

In particular, for your inclusion in a group insurance policy of the Company, the above mentioned data will be forwarded to the insurance company cooperating with the Company..... [insert name of the insurance company] which you will then contact yourself.

You reserve the right to withdraw your consent by making a request in the ways set out below.

Having taken note of the "Information of employees of the Company on the processing of personal data", as well as the above, I agree to the processing of my personal data for the stated purpose.

Full name.....

Address.....

Date.....

Signature/electronic signature

You may submit this by sending it to the e-mail address of the Company..... [insert e-mail of the Company] using your individual corporate email or in writing..... [insert Company postal address]. In this case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre (KEP) or a police authority.

5.3.5 Template of a prospective employee's declaration of consent

MODEL DECLARATION FOR THE CONSENT OF CANDIDATE EMPLOYEES

Our Company with the name..... and title ..... having its seat at ..... (street..... no. ..... tel..... e-mail: .....) collects and processes personal data of its potential employees, as Controller in accordance with Regulation (EU) 679/2016 (General Data Protection Regulation), because it is interested in hiring employees.

The personal data of candidate employees who were not recruited at the time of submitting their initial application shall be kept in accordance with the provisions set out below for the purpose of informing them about future employment opportunities in the Company.

The personal data collected and retained are a) your identification details, i.e. your name, father's name and mother's name, ID card number, gender, date and place of birth, nationality, b) your contact details, i.e. postal and email address, telephone number (landline, mobile), c) family status, education, CV, any disabilities, d) work history, professional experience, and e) reason for rejecting the recruitment application, e)..... [add any other data you process]

Your data will be retained by the Company for

1 year □ 2 years □

depending on your preference and will then be deleted/destroyed.

You reserve the right to withdraw your consent by submitting a request in the ways set out below.

Having taken note of the form 'Informing prospective employees of the Company about the processing of personal data', as well as the above, I agree to the processing of my personal data for the stated purpose.

Full name.....

Address.....

Date.....

Signature/electronic signature

You may submit this by sending it to the e-mail address of the Company..... [insert e-mail of the Company] or in writing to..... [insert the postal address of the Company]. In any case, in order to check your identity, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre (KEP) or a police authority.

5.4 Exercise of data protection rights and data subjects request handling procedure

5.4.1 Frequently Asked Questions about the exercise of the data subjects' rights

1) What are the rights of the data subject under the GDPR

The employee, customer or supplier, where he or she is a natural person whose personal data is processed by the controller, has a number of rights relating to the processing of the data, such as access to his or her data, rectification of inaccurate or incomplete data, erasure or objecting to the processing.

2) How is the right exercised?

It shall be exercised by submitting a written request to the controller, including by electronic means.

3) Can a fee be imposed and if so, under what conditions?

In principle, the exercise of the rights is free of charge. However, if the data subject's requests are manifestly unfounded or excessive, in particular because of their repetitive nature, the controller may levy a reasonable fee, taking into account the administrative costs of providing the information or communicating or carrying out the requested action. The controller shall bear the burden of proving the manifestly unfounded or excessive nature of the request.

4) What are the obligations of the SME as a controller?

The controller shall take appropriate measures to provide the data subject with any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 concerning the processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular where it concerns information specifically addressed to children.

The information shall be provided in writing or by other means, including, where appropriate, electronically.

Where requested by the data subject, the information may be given orally, provided that the identity of the data subject is proven by other means.

5) When should the SME respond (time constraints and possibility of extension)?

The controller shall provide the data subject with information on the action taken following his request without delay and in any event within one month of receipt of the request. That period may be extended by a further two months, if necessary, taking into account the complexity of the request and the number of requests.

The controller shall inform the data subject of such an extension within one month of receipt of the request and of the reasons for the delay.

Where the controller does not act on the data subject's request, the controller shall, without delay and at the latest within one month of receipt of the request, inform the data subject of the reasons for not acting and the possibility of lodging a complaint with a supervisory authority and bringing a judicial remedy.

6. When is the request considered complicated?

When it cannot be answered directly by the controller, but additional actions are also needed to satisfy him/her, in particular when further investigation by the controller or when other actors are involved in order to be answered and handled.

7. Can additional information be requested from the data subject (in particular for identification)?

Where the controller has reasonable doubts about the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

8. What happens when the applicant is *a minor*?

Such rights shall be exercised by the person exercising parental responsibility over the minor.

9. When does the SME have no obligation to fulfil the right?

- When it cannot establish the identity of the person making the request
- When the data subject's requests are manifestly unfounded or excessive, in particular because of their repetitive nature
- When the legal conditions for exercising and/or satisfying are not met

11. What happens if the right is not fulfilled? Further rights of subjects.

If the controller **rejects the request to fulfil the right,** the data subject shall have the possibility to lodge a complaint with the supervisory authority and to lodge a judicial remedy. The competent supervisory authority for Greece is the Data Protection Authority, Kifisias 1-3, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

5.4.2 Request form for the right of access

ACCESS REQUEST **(Article 15 GDPR)**
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....
SECTION ONE: Personal Details of Applicant
Applicant name..... Postal address

Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION TWO: Are you the data subject yourself?

☐YES
☐No-I submit the application on behalf of and in the name of the data subject.

A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Centre or a police authority.

B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens' Service Centre or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject
(if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Description of the request

Please fill in the corresponding fields:
A) Are you requesting confirmation for the processing?
(YES/NO)
B) Are you asking for information?
(YES/NO)
C) Do you request access to or a copy of specific data?
(YES/NO)
D) In case you request access to or a copy of your personal data, please describe which specific personal data you wish to obtain
.....
.....
.....
.....
.....
.....
.....
.....
.....

Please choose how you wish to receive your reply:

☐ Receive it by e-mail.....

☐ Receive it by post to your address

Street.....Number..... Area.....City.....
INFORMATION You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee. The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here. We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority. **Signature**..... **Date**.....
Attached documents 1) Identity documents of the data subject 2) Data subject identification documents in case submission of the application by a representative 3) Authorisation of the data subject to complete and submit the application by his or her representative 4) Supplementary documents relating to the access request

5.4.3 FAQ for the right of access

2.1. What is the right of access

The data subject has the right to request, *either in writing, electronically or orally (only upon his or her own request)*:

- Confirmation of any processing of its own data including specific information; and/or
- Receiving a copy of his/her personal data.

What information is provided:

Where the controller confirms such processing, the data subject shall have the right to receive further and the following information from the controller:

- ✓ the purposes of the processing;
- ✓ the categories of personal data concerned;
- ✓ the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

- ✓ where possible, the period of time for which the personal data will be stored or, where this is not possible, the criteria determining that period;
- ✓ the existence of a right to request the controller to rectify or erase personal data or to restrict the processing of personal data concerning the data subject or to object to such processing;
- ✓ the right to file a complaint to a supervisory authority;
- ✓ where personal data are not collected from the data subject, any available information on their origin;
- ✓ the existence of automated decision-making, including profiling, as well as important information on the logic followed and the significance and intended consequences of such processing for the data subject.
- ✓ the appropriate safeguards[83] that the DIRECT has received in accordance with Article 46 GDPR in case the data are transferred or transmitted to a third country or international organization.

2.2 In which cases can be exercised

The subject may exercise that right at <u>any time when</u>:

A) the controller processes his/her own personal data, and/or

B) it is not certain that processing takes place and the subject wishes to obtain confirmation from the controller, including the information referred to in point 2.1 above.

2.3. Obligations of the controller towards the subject following the request for access

A. Deadline for replying to the request

The controller should:

- *if it accepts the request,* **within one month** of the request to proceed with its satisfaction
- *if further investigation is needed*, it may request **an extension of up to a further two months**, explaining the reasons for it.

B. The controller must:

[83] In accordance with Article 46 GDPR, such appropriate safeguards may be provided through:(a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses issued by the Commission; (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (e) an approved code of conduct, in accordance with Article 40, together with binding and enforceable obligations of the controller or processor in the third country to apply appropriate safeguards; including as regards the rights of data subjects, or (f) an approved certification mechanism in accordance with Article 42 together with binding and enforceable obligations of the controller or processor in the third country to apply the appropriate safeguards, including as regards the rights of data subjects.

Provide **a** copy of the personal data, in principle free of charge, — *reasonable fee: if the request refers to more than one copy (see also section 1.3.)*

NOTE: The copy may also be provided in electronic form, if the request is made by electronic means, unless the data subject requests otherwise (e.g. mail).

and/or

confirm the existence of processing and provide relevant information requested.

2.4. Exemptions for satisfaction

The right to obtain a copy may not be satisfied if:

a) granting the subject adversely affects the rights and freedoms of third natural persons (e.g. professional secrecy). In such a case, the controller may satisfy the right following the deletion of contested personal data of third parties.

b) the request is manifestly unfounded or excessive, in particular because of its repetitive nature.

2.5. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the request, the controller shall inform the data subject thereof, in particular:

- a fully reasoned reply on the grounds for refusal, such as where it is manifestly unfounded or excessive, in particular because of its repetitive nature
- the right to lodge a complaint with the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- on the right to a judicial remedy

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

the data subject shall have the right to file a complaint to the Authority for the non-fulfilment of his or her right as well as to a judicial remedy.

5.4.4 Request form for the right to rectification

APPLICATION FOR THE EXERCISE OF THE RIGHT TO RECTIFICATION (Article 16 GDPR)
To Company name..... Postal address

Street……Number……Area……City……..
Tel……
Email…….
Application No/Date
.....

SECTION ONE: Personal Details of Applicant

Applicant name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION TWO: Are you the data subject yourself?

☐YES
☐No-I submit the application on behalf of and in the name of the subject data.

A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Service Centre or a police authority.

B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens' Service Centre or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject (if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Reasons for Rectification

Please indicate the specific reasons why you request the correction of your data by filling in the appropriate fields below and specifying in particular the correction or completion, respectively:

A) The data is incorrect:
.....
.....

B) My data is incomplete:
.....
.....

SECTION FIVE: Request description -Additional details

Please describe which specific personal data you wish to be corrected. In case you wish to submit additional documents relating to your request, please attach them to this application.

.....
.....

Please choose how you wish to receive your reply:
☐ Receive it by e-mail.....
☐ Receive it by post to the Address Street..... Number..... Area.....City.....
INFORMATION You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee. The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here. We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority. **Signature**..... **Date**.....
Attached documents 1) Identity documents of the data subject 2) Data subject identification documents in case submission of the application by a representative 3) Authorisation of the data subject to complete and submit the application by his or her representative 4) Supplementary documents relating to the rectification request

5.4.5 FAQ for the right to rectification

3.1. What is the right to rectification

The data subject shall have the right to require the controller without undue delay;

the *rectification* of inaccurate personal data concerning him/her; and

completion of incomplete personal data, including by means of a supplementary declaration

3.2. In which cases it can be exercised

Whenever the data subject considers his/her data to be incorrect or incomplete, i.e. they need to be completed to avoid misleading or misunderstanding

3.3. Obligations of the controller on the request

A. Deadline for replying to the request

The controller should:

- **within one month** of the request
- *if further investigation is needed*, it may request **an extension of up to a further two months**, explaining its reasons.

B. The controller must:

- promptly, without undue delay, comply with the request and in any case within the prescribed time limits;
- communicate to potential recipients of the data the rectification of such data, unless this proves impossible or involves disproportionate effort.

3.4. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the request, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- the grounds for refusal, such as where it is manifestly unfounded or excessive, in particular because of its repetitive nature;
- the right to file a complaint to the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- on the right to a judicial remedy

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to file a complaint to the Authority for the non-fulfilment of his or her right as well as to a judicial remedy.

5.4.6 Request form for the right to erasure

REQUEST FOR THE EXERCISE OF THE RIGHT TO ERASURE (Article 17 GDPR)
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....

SECTION ONE: Personal Details of Applicant

Applicant name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION TWO: Are you the data subject yourself?

☐YES
☐No-I submit the application on behalf of and in the name of the subject data.

A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Services Centre or a police authority.

B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens' Services Centre or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject (if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Reasons for Erasure

Please indicate the specific reasons why you request the deletion of your data by filling in the appropriate fields below:

☐**personal data are no longer necessary in relation to the purposes for which they were collected**
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐**withdraw your consent to the processing**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐**you object to the continued processing of your personal data**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐**do you consider that your personal data has been unlawfully processed**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐**there is an obligation by law to delete your data**

.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....

☐**you represent a minor and want personal data concerning him to be deleted from the Internet.**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

SECTION FIVE: Request description-Additional details

Please describe which specific personal data you wish to delete. In case you wish to submit additional documents relating to your request, please attach them to this application.

.....
.....
.....
.....
.....

Please choose how you wish to receive your reply:

☐ Receive it by e-mail.....

☐ Receive it by post to the Mail Directorate
Street..... Number.....
Area.....City.....

INFORMATION

You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee.

The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is

available here. We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority. **Signature……** **Date…….**
Attached documents 1) Identity documents of the data subject 2) Data subject identification documents in case submission of the application by a representative 3) Authorisation of the data subject to complete and submit the application by his or her representative 4) Supplementary documents relating to the erasure request

5.4.7 FAQ for the right to erasure

4.1. What is the right to erasure

Right to erase data from a file: The data subject shall have the right to request the controller to erase personal data relating to him or her from his/her record.

Right to be forgotten: A natural person (data subject) may request the operator of an internet search engine to delete one or more web links (containing published information about his/her face) from the list of results displayed after a search with his/her name. For example, he may request the deletion of a link with regard to an old newspaper article relating to a loan that has been repaid long ago. The operator of the search engine shall be obliged to delete the referred link if it is not a public person or where the general public interest in accessing the information does not outweigh the interests of the data subject.

More information is available on the Authority's website at: https://www.dpa.gr/el/polites/gkpd/dikaiwma_diagrafis/aitisi_diagrafis

4.2. In which cases it can be exercised

The data subject shall have the right to request the erasure of his or her data where:

- ✓ personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- ✓ the data subject withdraws his consent on which the processing is based and there is no other legal basis for the continuation of the processing.
- ✓ the data subject objects to processing pursuant to Article 21(1) and (2) GDPR and there are no compelling legitimate grounds for the processing
- ✓ the personal data have been unlawfully processed

- ✓ the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;
- ✓ when the data subject gave his/her consent as a child, he/she was not fully aware of the risks involved in the processing, and would later want to remove the personal data concerned, mainly from the Internet

4.3. Obligations of the controller on the request for erasure

A. Deadline for replying to the request

The controller should:

- if there is a legitimate reason for erasure, within one month of the request to proceed with the deletion of the data and inform the data subject thereof
- if further investigation is needed, it may request an extension of up to a further two months, explaining the reasons for it.
- In any case, it will have to respond to the request for deletion within three months of its submission.

B. Obligation to inform in the event of transfer to third parties

Where personal data are disclosed to third parties, the controller shall:

- communicate any erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves **impossible** or results to a **disproportionate effort**;
- where requested by the data subject, it shall inform the data subject of those recipients.

C. Obligation to inform controllers in case of disclosure.

The controller who made the personal data public, and is required to delete them, should inform the controllers processing those data that the data subject has requested that the controllers erase any links to those data or copies or reproductions of those data.

4.4. Exceptions to the satisfaction of right

The data subject shall not have the right to request the erasure of his or her data where processing is necessary:

- ✓ on the exercise of the right to freedom of expression and information
- ✓ to comply with a legal obligation
- ✓ for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (concerning cases where the controller is the public or public body)
- ✓ for reasons of public interest in the field of public health
- ✓ for archiving purposes in the public interest

- ✓ for scientific or historical research purposes or statistical purposes
- ✓ for the establishment, exercise or support of legal claims.

4.5. Satisfaction of right

If the right to erasure is satisfied by the controller:

- The fulfilment of the right to request deletion does not lead to the complete deletion of the data even if the links in question do not appear in the search engine result list.
- the original content is still accessible when other search criteria are used, other than the name, or is available on the original source website on which the posting was made

4.6. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

Where the data subject's request to delete his or her data is refused, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- the reasons for the rejection,
- the right to file a complaint to the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- the right to judicial redress.

B. Non-response to a request submitted

Where the controller or the search engine operator for the cases of the right to be forgotten does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to file a complaint to the Authority for failure to fulfil his or her right, as well as to a judicial remedy.

5.4.8 Request form for the right to restriction

REQUEST FORM FOR THE EXERCISE OF THE RIGHT TO RESTRICTION (Article 18 GDPR)
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....
SECTION ONE: Personal Details of Applicant

Applicant name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION TWO: Are you the data subject yourself?

☐YES
☐No-I submit the application on behalf of and in the name of the subject data.

A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Services Centre or a police authority.

B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens' Services Centre or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject (if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Grounds for Restriction

Please indicate the specific reasons why you request the restriction of the processing of your data by filling in the appropriate fields below:

☐ you question the accuracy of your data and ask for restriction of processing until it is verified by our company

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐ you consider processing unlawful and do not want your data to be erased, but to limit their use

.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐ your data is no longer necessary to us for the purposes of the processing, but you request their retention to establish, exercise or support legal claims

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐ you object to the processing in accordance with Article 21(1) and you are expected to verify whether the legitimate reasons of our business outweigh your reasons.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

SECTION FIVE: Request description -Additional details

Please describe for which specific personal data you wish to restrict the processing. In case you wish to submit additional documents relating to your request, please attach them to this application.

.....
.....
.....
.....
.....

Please choose how you wish to receive your reply:
☐ Receive it by e-mail.....   ☐ Receive it by post to the address   Street..... Number.....   Area.....City.....
INFORMATION   You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee.   The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here.   We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority.   **Signature ……..**   **Date…….**
Attached documents   1) Identity documents of the data subject   2) Data subject identification documents in case submission of the application by a representative   3) Authorisation of the data subject to complete and submit the application by his or her representative   4) Supplementary documents relating to the request for restriction of processing

5.4.9 FAQ for the right to restriction

5.1. What is the right to restriction

The data subject has the right to request the restriction of processing, i.e. the *temporary cessation* of the processing of his or her data, under specific conditions which are exclusively listed. When the right is satisfied, processing shall cease or be discontinued for a temporary period.

5.2. In which cases can be exercised

The data subject may request the restriction of processing where:

- ✓ questions the accuracy of his/her data until it has been verified by the controller;
- ✓ the processing is unlawful and the data subject objects to the erasure of the personal data and requests, instead, that their use be restricted;

- ✓ the controller no longer needs the personal data for the purposes of the processing, but such data are required by the data subject to establish, exercise or support legal claims;
- ✓ the data subject objects to the processing in accordance with Article 21(1) pending the verification of whether the legitimate reasons of the controller outweigh the data subject's reasons.

5.3. Obligations of the controller on the restriction request

A. Deadline for replying to the request

The controller should:

- **within one month** of the request to proceed with its satisfaction and inform the data subject thereof
- *if further investigation is needed*, it may request **an extension of up to a further two months**, explaining the reasons for it.

B. The controller must:

- satisfy the right to the prescribed time limits (see section 1.6.)
- limit processing in the following indicative ways:
  - i) transfer data temporarily to another system
  - ii) data should not be accessed by users
  - iii) data not temporarily published on the website

5.4. Results of the exercise of the right:

Temporary cessation of processing

***Attention*: possibility to continue processing, only:**

- i) with the consent of the data subject
- ii) for the establishment, exercise or support of legal claims
- iii) protecting the rights of other natural or legal persons
- iv) for reasons of important public interest of the EU or Greece

5.5. Exemptions for satisfaction

The controller may waive the right to restriction where it is manifestly unfounded or excessive, in particular because of its repetitive nature.

5.6. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the request, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- on the grounds for refusal, such as where it is manifestly unfounded or excessive, in particular because of its repetitive nature
- the right to file a complaint to the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- on the right to a judicial remedy

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to file a complaint to the Authority for failure to fulfil his or her right, as well as to a judicial remedy.

5.4.10 Request form for the right to data portability

APPLICATION FOR THE EXERCISE OF THE RIGHT TO PORTABILITY (Article 20 GDPR)
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....
SECTION ONE: Personal Details of Applicant
Applicant name..... Postal address Street……Number……Area……City…….. Tel..... E-mail.....
SECTION TWO: Are you the data subject yourself?
☐ YES ☐ No-I submit the application on behalf of and in the name of the data subject. A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens' Services Centre or a police authority.

B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens' Service Centre or a police authority, as well as the complete personal information (your and the data subject).

SECTION THREE: Personal details of the data subject
(if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Request Description

You wish to:

☐ to receive in person the personal data concerning you that you have provided to our Company as a controller and have been processed by automated means based on your consent or the contract between us in a structured, commonly used and machine-readable format.

☐ our Company to forward this information directly to another controller, if this is technically feasible, with the following information:

Controller's name:……..
Postal address:……
Street…….Number……..City……..Postcode
Telephone……Email…….

Please describe in detail your request as well as the type of data for which you are filing the request.
.....
.....
.....
……

In case you wish to submit additional documents relating to your request, please attach them to this application.
.....
.....
.....

Please choose how you wish to receive your reply:

☐ Receive it by e-mail.....

☐ Receive it by post to the Address
Street..... Number..... City.....Postcode…..

INFORMATION
You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large

number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee. The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here. We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority. **Signature**…….. **Date**……
Attached documents 1) Identity documents of the data subject 2) Data subject identification documents in case of submission of the application by a representative 3) Authorisation of the data subject to complete and submit the application by her or his representative 4) Additional documents on portability request

5.4.11 FAQ for the right to data portability

6.1. What is the right to portability

The right to portability offers individuals (data subjects) an easy way **to manage their personal data themselves**. It makes it **easier** for **them to move**, **copy** or transfer personal data from one IT environment to another.

Data subjects shall have the right to:

a) to receive their own personal data, which have been processed by automated means by a controller, in a structured, commonly used and machine-readable format

request that the controller transfer such data to another controller, without objection from the original controller. Where technically feasible, they may request that their data be transferred directly from one controller to another.

6.2. In which cases can be exercised

The right to portability may be exercised lawfully where the following cumulative conditions are met:

- ✓ The data are **processed** automatically on the basis of either the **consent** of the subject or the **performance of a contract** to which the data subject is a party;
- ✓ The data **must relate to and be provided by the data subject.** They are considered to be provided directly by the subject where (a) they are consciously and actively provided by the subject itself; or (b) produced and collected from the activities of users through the use of a service or device;

- ✓ The exercise of the right not to adversely affect the rights and freedoms of non-consensual data subjects. In order to prevent adverse effects on the third parties involved, processing by another controller shall only be permitted to the extent that the data remain under the control of the requesting user and that its management meets exclusively personal or domestic needs.

6.3. In which cases it cannot be exercised

The right to portability cannot be exercised:

- ✓ Where the right to erasure has previously been exercised
- ✓ Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.4. Obligations of the controller on the portability request

A. Deadline for replying to the request

The controller should:

- **if it accepts the portability request** within one month of the request to proceed with its satisfaction and inform the data subject thereof
- if further investigation is needed, it may request an extension of up to a further two months, explaining the reasons for it.
- in any case, it should reply to the request within three months of the submission of the request.

B. Further obligations of the controller

- Has an obligation to check and verify that the data are accurate and up-to-date before transmitting them to the controller to be designated by the data subject;
- Acts on behalf of the data subject, including in the case of transfer of the data directly to another controller, in which case he or she is not responsible for compliance with the data protection law of the receiving controller.

6.5. Satisfaction of the request

If the request is accepted, the controller shall:

- transmit the requested data directly to the controller designated by the data subject; or
- where the data subject has requested it, it shall provide him/her with the relevant information.

6.6. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the data subject's request, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- the reasons for the rejection, and
- that he/she has the right to lodge a complaint with the Authority for failure to fulfil his or her right and the right to a judicial remedy.

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to file a complaint to the Authority for failure to fulfil his or her right.

5.4.12 Request form for the right to object

APPLICATION FOR THE EXERCISE OF THE RIGHT TO OBJECT (Article 21 GDPR)
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....
SECTION ONE: Personal Details of Applicant
Applicant name..... Postal address Street……Number……Area……City…….. Tel..... E-mail.....
SECTION TWO: Are you the data subject yourself?
☐YES ☐No-I submit the application on behalf of and in the name of the data subject . A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre or a police authority. B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens Service Centre or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject
(if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Grounds for Objection

Please indicate the specific reasons why you request the objection of the processing of your data by our Company and the types of personal data related to the request:

.....
.....
.....
.....
.....

SECTION FIVE: Additional information

In case you wish to submit additional documents relating to your request, please attach them to this application.
.....

Please choose how you wish to receive your reply:

☐ Receive it by e-mail.....

☐ Receive it by post to the Address
Street..... Number.....
Area……..City.....

INFORMATION

You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee.
The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here.
We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority.

Signature……
Date…….

Attached documents
1) Identity documents of the data subject

2) Data subject identification documents in case submission of the application by a representative
3) Authorisation of the data subject to complete and submit the application by his or her representative
4) Supplementary documents relating to the objection request

5.4.13 FAQ for the right to object

7.1. What is the right to object

The data subject shall have the right to object at any time and for reasons relating to his or her particular situation to the processing of personal data relating to him or her.

7.2. In which cases can be exercised

The right may be exercised at *any time* when the processing is based on:

- ✓ the performance of a task in the public interest, or
- ✓ the existence of a legitimate interest of a third party or of the controller; or
- ✓ the above bases and profiling takes place

7.3. Obligations of the controller on the objection request

A. Deadline for replying to the request

The controller should:

- within one month of the request to proceed with its satisfaction and inform the data subject thereof
- if further investigation is needed, it may request an extension of up to a further two months, explaining the reasons for it.

B. The controller must:

- stop editing
- **immediately** stop processing if it is ***for marketing purposes***

7.4. Exemptions

The controller shall not be obliged to satisfy the right to object in the following cases:

- ✓ if it demonstrates compelling legitimate grounds for processing which take precedence over the interests, rights and freedoms of the data subject; or
- ✓ in order to establish, assert, or support his legal claims.

7.5 Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the data subject's request, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- the reasons for the rejection, and
- the right to file a complaint to the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- the right to judicial redress.

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to file a complaint to the Authority for failure to fulfil his or her right, as well as to a judicial remedy.

5.4.14 Request form for the right not to be subject to automated individual decision-making/profiling

APPLICATION FOR THE EXERCISE OF A RIGHT NOT TO BE JUBNECT TO AUTOMATED INDIVIDUAL DECISION-MAKING/PROFILING (Article 22 GDPR)
To Company name..... Postal address Street……Number……Area……City…….. Tel…… Email……. Application No/Date .....
SECTION ONE: Personal Details of Applicant
Applicant name..... Postal address Street……Number……Area……City…….. Tel..... E-mail.....
SECTION TWO: Are you the data subject?
☐YES ☐NO-I submit the application on behalf of and in the name of the data subject. A) In the event that you are the data subject yourself, please attach a copy of your ID card, passport or any other document certifying your identity, certified by a Citizens Service Centre (KEP) or a police authority. B) In case you act as a representative of the data subject, please attach a copy of the data subject's authorisation, validated by a Citizens Service Centre (KEP) or a police authority, as well as the complete personal information (yours and the data subject's).

SECTION THREE: Personal details of the data subject
(if the subject is not the applicant)

Data subject name.....
Postal address
Street……Number……Area……City……..
Tel.....
E-mail.....

SECTION FOUR: Request description

A) Please describe why you wish not to be subject to a decision taken solely on the basis of automated processing, including profiling and what this decision is.
.....
.....
.....
.....
B) Please indicate why you request human intervention from our Company.[84]
.....
.....
.....
.....
In case you wish to submit additional documents relating to your request, please attach them to this application.
.....
.....

Please choose how you wish to receive your reply:

☐ Receive it by e-mail.....

☐ Receive it by post to the Postal Address
Street.....Number.....
Area……City.....

INFORMATION
You will receive a reply to your request free of charge without delay, and in any case within (1) one month after we receive this application. However, in the event that your request is complex or there is a large number of your requests, we will inform you within the month if we need to receive an extension of another (2) two months within which we will reply. If your requests are manifestly unfounded or excessive due in particular to their repetitive nature, our company may charge a reasonable fee.
The personal data you provide through this Application are processed by our Company for the purpose of examining your request regarding the protection of your personal data (as required by Regulation 679/2016/EU). Access to these data may have processors on behalf of our company, more information is available here.

[84] To be completed where the decision taken on the basis of automated processing by the controller is (a) necessary for the conclusion or performance of a contract between the data subject and the controller or (b) is based on the data subject's explicit consent. In such cases, you have the right to have human intervention on the part of the controller, express an opinion and challenge the decision.

We do not reply by using automated decision-making. You have the rights to access, rectify, erase, and restrict processing and, in case your request is not satisfied, you have the right to submit a complaint to the Authority. **Signature……** **Date……..**
Attached documents 1) Documents identifying the data subject 2) Data subject identification documents in case submission of the application by a representative 3) Authorisation of the data subject to complete and submit the application by his or her representative 4) Supplementary documents relating to the request for non automated processing and/or profiling

5.4.15 FAQ on the right not to be subject to automated individual decision-making/profiling

8.1. What is the right

In order to lawfully process automated data – including profiling – controllers must respect the principles of fair processing and have a lawful basis for processing.

In this context, they ensure the transparency of the processing by providing information to data subjects, minimising their personal data, ensuring that they are accurate, verifying them, following the appropriate retention times and updating them on a regular basis. In particular, they should be able to justify the need to collect and use personal data for profiling for the purpose of processing they seek each time, otherwise they have to choose anonymised or pseudo — anonymised data.

In particular for a decision which produces legal effects concerning the subject or significantly affects the subject, by an exclusively automated method, including profiling, the following shall apply:

- The controller may lawfully take such a decision, in accordance with Article 22(2) GDPR, only if the subject has given explicit consent or where the decision is necessary for the conclusion or performance of a contract between a data subject and a controller or that decision is authorised by the Union or Member State law to which the controller is subject and which provides for appropriate measures to protect the rights of the data subject.
- If that decision was taken as necessary for the conclusion or performance of a contract between the controller and the subject or on the basis of the explicit consent of the subject, the latter shall **have the right to challenge it** and the controller shall be obliged to implement appropriate measures to protect his or her rights, such as ensuring **human interference** in the decision-making or **the right to express an opinion** and **contesting the decision** by the subject.

- Where the controller carries out automated processing of data, including profiling, it shall provide the data subject, at the time of receipt of the data (when it has collected it from the data subject) or within a reasonable time (when received from another source), in addition to the information contained in Articles 13 and 14 GDPR, the following **additional information:**
  - ✓ whether and to what extent automated decision-making is taking place, including profiling;
  - ✓ the logic involved,
  - ✓ the significance and envisaged consequences of the processing,
  - ✓ at the latest at the time of the first communication with the data subject, the controller shall indicate the right of the data **subject to object** which is **clearly and separately** described from any other information.

In many cases, the data subject **has the right to prevent automated data processing**.

Automated individual decision-making

The procedure concerns decisions taken without human intervention, such as an electronic decision taken after the submission of an application for a loan.

Profiling

Profiling requires the use of personal data to analyse or predict data, such as performance at work, economic situation, health, personal preferences and interests. Profiling information is obtained from various sources, such as internet searches, shopping habits, social networks and lifestyle data received from mobile phones.
The data subject shall have the right to:

- object to a decision based solely on automated data processing if this decision affects its legal rights or other equally important issues (e.g. automatic rejection of an online loan application or e-recruitment practices without human intervention)
- understand the reasons why decisions concerning him or her are taken by automated processing and their possible consequences;
- object in some cases to profiling, including direct marketing.

If these three situations exist, the data subject shall have the right at any time to request the CONTROLLER (a) not to undergo automated processing and (b) to explain the reasons why a decision was taken in this way.

8.2. In which cases it can be exercised

- ✓ In exclusively automated processing
- ✓ In cases of profiling

8.3. Obligations of the controller on the request

Time limit for replying to the request

- **if the request is accepted,** within one month of its submission, the controller should respond to the request and inform the data subject thereof
- if further investigation is needed, the controller may ask for an extension of up to a further two months, explaining the reasons for it.

8.4. Satisfaction of rights

If the request is accepted:

- the controller no longer submits the data to automated processing
- if the basis for profiling is the consent of the subject and it is revoked or the subject exercises the right to erase his or her data under Article 17 GDPR, the controller **is obliged to delete** the personal data concerned, unless there is another legal basis for processing, in accordance with the provisions of the Regulation.
- where the data subject objects to automated processing of his or her data, including profiling, the controller shall no longer process the personal data, unless it demonstrates compelling legitimate grounds for processing which take precedence over the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- where data subjects object to the processing of their personal data for **direct marketing** purposes, such data shall no longer be processed for those purposes.

8.6. Exemptions to the satisfaction of rights

The controller should not take decisions based solely on automated data processing where such decisions affect the legitimate rights of the data subject or other equally important matters, unless:

- ✓ such decisions are necessary for the conclusion or performance of a contract;
- ✓ it is authorised by the law of the Member State which provides for appropriate measures to protect the rights, freedoms and legitimate interests of the subject
- ✓ there is a prior explicit consent of the subject

8.5. Rejection of a request – Non-response to a submitted request

A. Rejection of a request

In the event of rejection of the data subject's request, the controller shall inform the data subject in a fully reasoned reply thereof, in particular:

- the reasons for the rejection, and
- the right to lodge a complaint with the Authority (with reference to the contact details of the Authority) for failure to fulfil his/her right, and
- the right to judicial redress.

B. Non-response to a request submitted

If the controller does not reply to the request within the legal deadline, or its response is unsatisfactory:

- the data subject shall have the right to lodge a complaint with the Authority for failure to fulfil his or her right.

5.5 Destruction of personal data

5.5.1 Frequently Asked Questions about the destruction of a personal data file

1. What is file destruction (is this file the same as the Article 30 GDPR file?)

The destruction of a file shall also constitute a processing operation as provided for in Article 4(2) of the GDPR, which as such is also subject to the rules governing any processing of personal data in Article 5 GDPR. Thus, any file containing personal data must be lawfully destroyed, after the time required to fulfil the purpose, for which it has been collected and carried out safely, in such a way that it cannot be retrieved after its destruction and identified with a particular natural person.

The personal data file is not identical to the record of processing activities under Article 30 GDPR. The former shall cover any personal data subject to automated processing or to non-automated processing of data contained or to be included in a filing system. On the other hand, the second includes only the information (although not exhaustively listed) of the processing activities referred to in Article 30(1) and (2) GDPR. The personal data file is therefore broader than the record with the processing activities of Article 30 GDPR.

2. Why do the files have to be destroyed?

Files with personal data shall be governed by the rules for the processing of personal data. A basic rule is the principle of limitation of the storage period, which dictates that personal data will not be retained permanently but will be destroyed when the reason for their collection ceases, i.e. when the purpose for which they were collected has ended.

Furthermore, the destruction of files minimises the risk of breaches for an SME, i.e. security breaches that may lead to unlawful disclosure or access to personal data by third parties, non-qualified persons or organisations.

3. Who has an obligation to destroy?

The obligation to destroy is the responsibility of the controller, who must implement a specific procedure to ensure that the data have been destroyed in a secure manner.

In addition, where the destruction of files is entrusted by the controller to a processor, a natural or legal person, there must be a written contract of entrustment between them, describing the essential elements of the destruction. In the event of circumvention, this contract serves, in the context of the accountability of Article 5(2) GDPR, to demonstrate compliance with the institutional framework for the protection of personal data and the attribution of responsibilities between controllers and processors, and to establish civil claims between them.

4. What rules apply to the destruction of files?

When destroying files, every SME must take into account the principles of limiting the storage period in Article 5(1)(e) GDPR and the security of data that guarantees their protection against unauthorised or unlawful destruction of Article 5(1)(f) GDPR.

The first principle dictates that personal data must be destroyed immediately after the end of the period required to carry out the purpose of the processing.

The second principle requires that personal data must be destroyed in a secure manner so as to exclude further unlawful processing, such as any form of making available to third parties, and that their destruction is irreversible, i.e. it cannot be retrieved after destruction by technical or other means, so that the data subjects can be identified.

5. When is the file being destroyed?

The institutional framework for personal data does not provide for any specific timeframes or deadlines within which personal data contained in a filing system must be destroyed.

Therefore, each SME must determine the time of destruction of the files of the personal data it keeps and processes itself. The destruction and timing of such destruction may be included in the data retention policy that each SME maintains and follows.

In determining the time of destruction of files, two factors are taken into account: a) the purpose of processing, after which there is no need to maintain them, and b) the existence of any legal or other claims (tax, insurance, etc.) that dictate their preservation beyond the realisation of the purpose of processing. In the latter case, the

time (e.g. 1 year, 5 years, or 10 years) must be explicitly specified by the SME in its data retention policy (documentation).

6. How do they get destroyed?

The choice of how to destroy is left to the SME as the controller. When choosing how, each SME should ensure that personal data is safely destroyed to exclude further unlawful processing and that it cannot be retrieved after its destruction.

The choice of how to securely destroy personal data depends on the means used to keep and further process the data.

Finally, where the destruction of files is technically and/or organisationally difficult for the SME, as the controller, it may be entrusted in writing to a third party, natural or legal person, who will take over the destruction in its name and on its behalf (processor).

7. Is there a distinction between paper and electronic files in terms of their destruction?

The safe destruction of personal data files shall take into account the means used to maintain and further process them. Personal data held in printed/paper form may be safely destroyed by cutting into strips, mashing and recycling or burning, while data held in electronic form may (a) be replaced by overwriting, using special programs (file erasers, file shredders, file pulveritisers), b) destroyed by formatting the substrate material (format), or c) physical destruction of the material substrate itself (e.g. by crushing, pulverising or cremating).

5.5.2 Template of a File Destruction Policy

1. Purpose

Our company by the name.....[85] (and distinctive title[86].....) established in..... (street....., no. …… tel..... e-mail: .....) destroys the personal data of employees, prospective employees, customers, suppliers and visitors that it keeps in printed/paper and electronic form in order to carry out its professional activity in accordance with the regulatory framework for the protection of personal data as established by GDPR 2016/679 and Law 4624/2019 and as specialized in the directives and decisions of the Data Protection Authority.

The destruction of personal data also constitutes processing, as referred to in Article 4(2) GDPR, which consists of the conversion of personal data into non-personal data and which is itself subject to the personal data protection rules, as resulting from the GDPR and specified in particular by the Authority's Directive 1/2005.

[85] *Complete full legal name or name in case of sole proprietorship.*
[86] *Fill in the distinctive title (trade name) of the company, if any.*

The purpose of the policy is to define the conditions required to comply with the regulatory framework for the protection of personal data relating to their destruction after the fulfilment of the purpose of the processing.

2. Scope

This policy concerns all personal data held and processed by the company. It includes personal data relating to the following as data subjects:

- ✓ Employees
- ✓ Prospective employees
- ✓ Customers
- ✓ Suppliers
- ✓ SME Visitors

In addition, the destruction policy concerns personal data:

- ✓ included in filing systems (paper files) or
- ✓ processed by automated means (electronic files)

and extends to the completion of the "life cycle" of personal data, i.e. until the end of the period needed for the purpose of processing (Article 5(1)(e) GDPR).

The destruction policy does not cover cases where personal data are retained for a longer period in order to be processed for filing purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1) GDPR.

3. General principles of destruction

Taking into account the principle of limitation of the storage period (Article 5(1)(e) GDPR), after the completion of the processing of personal data (based on the principles of lawfulness and purpose limitation set out in Article 5(1)(a) and (b)) the company destroys them in a secure manner, taking appropriate organisational and technical measures, so that after the destruction it would not be possible to identify the data subjects and their further unlawful processing, such as any form of disclosure to third parties, can be excluded.

4. Categories of personal data to be destroyed

Depending on the means used for the retention and further processing, personal data are divided into:

a) data in printed form (e.g. documents).

b) data in electronic form held on any physical substrate (hard computer discs, CDs, DVDs, usb, etc.). These data may be either in a structured format (e.g. a database), or form a set of individual computer files (e.g. text files, images, etc.).

c) data in another form (e.g. data held on video cassettes, microfilm, etc.).

5. Case of entrustment of the destruction to processors

Destruction, in particular in cases of large files, for which appropriate technical equipment is required, may be entrusted to a company which, as processor, may be ordered by the controller (Article 4(8)) to undertake on its behalf the destruction of the files.

The relevant assignment to a processor must be made by means of a contract specifying:

- ✓ the measures to be implemented by the processor for the secure transfer of the data to the place of destruction;
- ✓ the place of destruction,
- ✓ any intermediate storage sites for the data;
- ✓ the way of destruction,
- ✓ the maximum time allowed from the time of delivery of the data by the controller to the processor until their final destruction.
- ✓ any additional instructions from the controller regarding technical and organisational destruction measures;
- ✓ the exact details of any third parties (subcontractors) who are to carry out part or all of the destruction of the data on behalf of the processor.

Finally, where personal data to be destroyed are subject to confidentiality (e.g. medical confidentiality), the company in principle carries out the destruction itself, in order to avoid unfair access to confidential data by third parties. In cases where this is technically and/or particularly difficult for the company, the assignment to a processor shall be carried out in such a way that the company has overall supervision of the destruction process (e.g. that the data are destroyed within the controller's premises), or if this is not possible (e.g. where the data are kept in printed form) an authorised person of the company supervises the destruction of the data at the processor's premises.

6. Time of data destruction

Depending on the period required to carry out the purpose of the processing, the personal data shall be destroyed:

A) daily: This case concerns personal data produced and/or used daily in the context of the SME's work and which, after carrying out the specific work, are useless (in paper and/or electronic form). Where temporary storage of such data is deemed necessary, it shall not exceed a reasonable period of time on a case-by-case basis. Especially when data digitisation takes place e.g. scanning, original files in paper form should be destroyed.

(B) scheduled: The case concerns a mass destruction of data that takes place either because the period required to carry out the purpose of the processing (according to the applicable data retention time) has elapsed for the data concerned, or for other reasons, such as cessation or modification of operations of the controller or the lack of infrastructure for safe daily destruction.

In the case of the scheduled destruction, it is appropriate to carry out a periodic check (e.g. every 3 and 6 months) in order to determine whether the reason for the existence of the personal data has ceased to exist during that period and that it is therefore necessary to destroy them.

7. How to destroy data in paper form

A secure procedure for the daily or scheduled destruction of personal data held in paper form (documents) includes the following steps:

- ✓ Collection of documents to be destroyed by SME employees in special receptacles located at specific locations within its premises where access is controlled
- ✓ If there is the possibility to digitise documents (scanning and digitisation) and there is an infrastructure for their daily destruction (shredder), the company must cut the documents (e.g. into strips) at its premises and then recycle them.

8. Entrusting destruction to a processor

If the company is not able to destroy the documents at its premises, it may entrust the processing of the destruction, in writing, to a specialised external partner (processor). In this case, it must:

1) complete a protocol for the delivery of data to the partner responsible for the destruction;

2) receive from the processor a data destruction protocol after the destruction

3) the contract between controller and external partner should specify:

- ✓ the measures to be implemented by the external partner for the safe transfer of data to the place of destruction;
- ✓ the place of destruction,
- ✓ any intermediate storage sites for the data;
- ✓ the way of destruction,
- ✓ ensuring the confidentiality of data, as well as
- ✓ the maximum time allowed between the time of delivery of the data and the final destruction of the data.

In addition, an authorised employee of the company may supervise the destruction of the data at the external partner's premises, in particular in the case of confidential data. Documents may be destroyed by cutting, mashing or burning (in an incinerator with appropriate permits). After cutting, pulping and/or recycling of documents may be followed.

9. How to destroy data held in electronic form

For the safe destruction of personal data in electronic form it is not sufficient simply to delete it (e.g. with the command "DELETE"), as this only deletes the reference to the data, while the data itself may be recoverable using special software programs.

The appropriate way to safely destroy personal data stored on rewritable media (e.g. hard drives, rewritable DVDs and CDs) is to alter the data by replacing them with overwrite. The alteration can be done using special programs (file erasers, file shredders, file pulveritisers). In the case of daily data destruction, an alternative way of destruction is to format.

In the case of the scheduled destruction of all data, an alternative means of destruction (for particularly critical data) is also the natural destruction of the material medium itself (e.g. by fragmentation, pulverisation, incineration, without prejudice to specific provisions on special waste management/environmental protection).

The destruction of data includes the destruction of all backups kept by the company.

The scheduled destruction of the data must be accompanied by a destruction protocol.

10. Destruction registration — protocol and information

The data destruction protocol includes (at least) the following elements:

- ✓ Date of data destruction
- ✓ Description of the personal data destroyed
- ✓ Method of destruction
- ✓ Name of the employee of the company responsible for the destruction
- ✓ Processor of the destruction (in case the destruction is delegated to a processor).

The destruction protocol shall be maintained safely under the responsibility of the company.

5.5.3 Template of a File Destruction Protocol

TEMPLATE OF A FILE DESTRUCTION PROTOCOL
The following personal data were safely destroyed in accordance with the Company's destruction policy and in compliance with the personal data protection regulatory framework
Controller[87] The Company bearing the name.....[88] (and distinctive title[89].....) established in..... (street....., no. ……. tel..... e-mail: .....)

[87] Complete the full name of the company.
[88] *Complete full legal name or name in case of sole proprietorship.*
[89] *Fill in the distinctive title (trade name) of the company, if any.*

Date of destruction	**Responsible employee of the Controller**
Description of the personal data destroyed	
Method of destruction Incineration Cutting Pulp Overwrite Format Physical destruction of equipment Other: —	
In case the processing is to be carried out on behalf of a controller[90], the destruction was carried out by:	
Processor:	
Responsible employee of the Processor:	

[90] Complete the full details of the processor as indicated in the delegation contract.

5.6 Records of processing activities

5.6.1 Frequently Asked Questions for the records of processing activities

1. What is a record of processing activities?

A record of the processing activities is the record containing the information provided for in Article 30 of the GDPR with regard to the activities carried out by each micro, small and medium-sized enterprise (SME) and related to the processing of personal data in the course of the business with a view to carrying it out.

Under the GDPR as of 25 May 2018, records of processing activities are kept internally by businesses and made available to the supervisory authority upon request (Article 30(4) GDPR).

2. What is the relationship between the record of processing activities and the previous institutional provision of file notification?

The concept of a record of processing activities is not unknown to the Greek institutional framework for the protection of personal data. Both Directive 95/46/EC and Law 2472/1997 provided for a general obligation to disclose to the supervisory authority personal data records and to obtain permission for those files, which included sensitive data. Experience with the implementation of the previous institutional data protection framework at European but also at national level has shown that this obligation has not effectively contributed to improving the level of protection of personal data[91]. And although the submission of a notification to the supervisory authority and the authorization of the supervisory authority, where required, serves as a presumption of compliance by companies with the requirements of the personal data protection rules, now as of 25 May 2018, when the aforementioned obligation to notify and obtain authorization from the supervisory authority has been abolished,[92]companies in accordance with the general principle of accountability laid down in Article 5(2) of the GDPR must establish and maintain records of processing activities that comply with the general principles of processing set out in Article 5(1) GDPR and demonstrate their compliance with these principles. Passing on the burden of proof of compliance from the supervisory authority to companies cannot and should not be perceived by companies as weakening of the personal data protection rules.

3. What is processing activities?

The GDPR does not provide a definition of processing activities. Article 4, point 2 defines 'processing' as any operation or set of operations carried out, whether or not by automated means, on personal data or on sets of personal data, such as:

- collection;

[91] See Recital 89 GDPR

[92]See Recital 89 GDPR and Authority Decision 46/2018, available at www.dpa.gr

- registration;
- organisation;
- structure,
- storage,
- adjustment or change;
- recovery;
- searching for information;
- use;
- disclosure by transfer;
- dissemination or any other form of making available;
- association or combination;
- restriction;
- erasure or destruction.

The frequent use of the terminology “processing activities” in different provisions of the GDPR (Articles 24(2), 35(6) and 10, 40(6) and 7, 42(6) and 60(10)) shows that this concept is broad and is not limited to the above list of individual processing activities. Each processing activity may include individual processing operations carried out for a certain purpose.

Advice: Each company must specify the intended purpose of any processing of personal data carried out by it.

4. What is the significance of the activity record?

By establishing and keeping a record of its processing activities, each company organizes its operational activities more effectively, while ensuring transparency of the personal data it processes. In doing so, it builds its legal toolbox for the type of personal data of employees, suppliers and customers that it further collects and processes (maintains, transfers or deletes), the purpose for which it processes them, the legal basis it uses and the rules it follows for its individual processing operations. According to Recital 82 of the GDPR and based on the accountability principle of Article 5(2) GDPR, activity records serve as a presumption of compliance with the requirements established by the GDPR.

In addition, for those businesses for which the designation of a Data Protection Officer (DPO) is mandatory (Article 37(1) GDPR), activity records assist his/her work in monitoring compliance with the GDPR and, in particular, in raising awareness and training of employees involved in processing operations, in accordance with Article 39(1)(b) GDPR.

Finally, through the records, companies are able to confirm/verify internally, but also to demonstrate to the supervisory authority that they have fulfilled the requirements of the GDPR. The obligation to display to the supervisory authority the company's records stem not only from the specific provision of Article 30(4) GDPR, but is part of the general obligation to cooperate with the supervisory authority in the performance of its tasks under Article 31 GDPR.

Importance of records

- ✓ **Compliance with GDPR (Recital 82, Art. 30 and 5(2) GDPR)**
- ✓ **Assisting the DPO's work (Art. 39(1)(b) GDPR)**
- ✓ **Demonstration to the supervisory authority (Articles 30(4), 31, 58(1)(e) and 83(5)(e) GDPR)**

5. Who has an obligation to keep a record of processing activities?

According to the provision of Article 30 GDPR, each controller, processor and, where applicable, their representatives, are required to keep a record of the processing activities for which they are responsible. Therefore, when keeping and processing records of personal data processing activities, each company falls under the obligation to keep that record.

Where two or more companies jointly determine the purpose or purposes of the processing of personal data and carry out processing of personal data and/or jointly determine the means they use for the processing, i.e. acting as joint controllers, then this obligation is not imposed on each company individually. In such a case, it may be agreed between them who bears this obligation established by the GDPR.

Furthermore, where a company acting as a controller or processor does not have its establishment in the Union, but has appointed a business as a representative in the Greek territory, then the representative is required to comply with Article 30 GDPR.

6. Who is exempt from the obligation to keep the record?

According to the provisions of Article 30(5) GDPR, the obligation to keep records does not concern companies employing fewer than 250 persons. The exception to this obligation stems from the intention of the EU legislator to reserve a more flexible approach to micro, small and medium-sized enterprises due to their specific situation in general to the application of the rules stemming from the GDPR, in particular the obligation to keep records[93].

[93] According to Recital 13 GDPR "(...) *To take account of the specific situation of micro, small...". In order to take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organizations employing fewer than 250 persons as regards record keeping. In addition, the Union institutions and bodies, as well as the Member States and their supervisory authorities, are encouraged to take into account the specific needs of micro, small and*

The concept of micro, small and medium-sized enterprises is defined in accordance with Article 2 of the Annex to Commission Recommendation 2003/361/EC as follows:

1. The category of micro, small and medium-sized enterprises (SMEs) consists of enterprises which employ fewer than 250 persons and whose annual turnover does not exceed EUR 50 million or whose annual balance sheet total does not exceed EUR 43 million.

2. In the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million.

3. In the SME category, a micro-enterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover or annual balance sheet total does not exceed EUR 2 million.

7. Is the exemption from the obligation to keep an activity record absolute?

The exemption from the record-keeping obligation is not absolute. According to the provision of Article 30(5) GDPR, three exceptions are introduced, under which micro, small and medium-sized enterprises employing fewer than 250 persons still have to keep records of their processing activities, i.e. where:

a) the processing carried out is likely to pose a risk to the rights and freedoms of the subjects;

b) the processing is not occasional and

c) the processing includes special categories of data as referred to in Article 9(1) GDPR or processing of personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

The complexity of the wording of this provision, taking into account the specificities and requirements of the modern digital era, shows that in practice very few companies could benefit from the exemption from the obligation to keep records.

In particular, the first exemption from the obligation to keep records of processing activities concerns SMEs, as controllers or processors, which carry out processing which is likely to pose only a risk, rather than a high risk, to the rights and freedoms of data subjects. Furthermore, the concept of risk to the rights and freedoms of data subjects is linked to several obligations established by the GDPR, such as the appropriate organizational and technical measures that the controller has to implement to demonstrate that the processing is carried out in accordance with the GDPR (Article 24(1)), the measures to protect personal data by design and by default (Article 25(2)) and the obligation to notify the supervisory authority in case of a breach of personal data (Article 33).

In addition, with regard to the second exception, SMEs are likely to systematically process — and not occasionally — personal data of their employees and/or their suppliers. According to the Article 29 Working

medium-sized enterprises when applying this Regulation. The concept of micro, small and medium-sized enterprises should be based on Article 2 of the Annex to Commission Recommendation 2003/361/EC".

Party, a processing activity may be considered occasional where it is not carried out systematically and is outside the normal business activities of controllers and processors[94].

Finally, many SMEs are likely to process a specific category of personal data (Article 9 GDPR, e.g. health data) or data related to criminal convictions and offences (Article 10 GDPR) for example for the purpose of staff management/administration and therefore cannot benefit from the exception of Article 30(5) GDPR.

In any case, SMEs should not confuse other obligations under the GDPR to be exempted from the obligation of Article 30 GDPR. For example, the fact that private doctors are exempted from the obligation to designate a DPO[95] cannot be used as a criterion for exempting them from the obligation to keep records of processing activities, since they systematically process special category data (health data) of their patients-customers.

Advice

- ✓ **The numerical criterion of 250 employees is not in itself sufficient to exempt SMEs from the obligation to keep records of processing activities.**
- ✓ **Exceptions introduced in Article 30(5) on exemption from the obligation to keep records of processing activities should be considered by each SME with particular care.**

8. What is the role of the DPO in drafting and maintaining the record?

The obligation to keep records of processing activities lies with the controller and the processor. This obligation does not fall within the remit of the DPO, nor is the DPO obliged to lay down specifications relating to these records. However, taking into account the tasks of the DPO, and in particular the advice to the controller and the processor on the obligations under the GDPR (Article 39(1)(a)), the monitoring of compliance with the GDPR, but also the duty to raise awareness and training of employees involved in the processing operations (Article 39(1)(b) GDPR), SMEs may entrust the DPO with keeping records of processing activities under his/her supervision[96].

9. What is the content of the record?

The content of the record with the processing activities varies according to whose obligation is to prepare and maintain it, i.e. (a) the controller, and where applicable its representative and b) the processor and its representative.

[94] See WP29 Guidelines on Article 49 of Regulation 2016/679 (WP262).
[95] See WP29 Guidelines on Data Protection Officers DPOs (WP 243 rev. 01., 2.1.3).
[96] See Article 29 Working Party, Guidelines on Data Protection Officers, from 13.12. 2016 (WP 243 rev. 01., 2.1.3), pp. 25-26.

Both the additional information concerning the purposes of the processing and the categories of recipients (Article 30(1)(b) and (d)) and that of the categories of data subjects and categories of personal data (Article 30(1)(c)) which the SME, as the controller, must include in the record with the processing activities, unlike the SME, acting as processor, are linked to the different role played by these two actors, both controller and processor, in the processing of personal data.

In addition, the information to be included in the records with the processing activities is not exhaustive. For example, when an SME in the course of its business also carries out research, even occasionally and not systematically, it should include the processing of personal data for this purpose in the record of the processing activities.

Finally, much of the information to be included in the record on processing activities is information that should be provided by the SME, as the controller, to the data subject, when exercising the rights of information and access (Articles 13, 14 and 15 GDPR).

This is an additional reason for proper training and record keeping, which can effectively achieve the fulfilment of the rights of the subjects. In addition, the controller's response to the rights of the data subjects (e.g. employees, suppliers) should also be included in the record of processing activities, as it alone constitutes processing of personal data.

- ✓ **The information contained in the activity records is different for controllers and processors.**
- ✓ **The list of information to be included in the records of activities is not exhaustive.**
- ✓ **The record of processing activities assists controllers in fulfilling the rights of the subjects.**

Checklist

- ✓ SME activity e.g. health, education, tourism, retail
- ✓ Intended purposes of any processing e.g. personnel management/administration
- ✓ Processing purposes involving processing activities.

10. What should SMEs take into account when creating records (which rules/principles should be respected/fulfilled)?

A) Controller

Article 30(1)	Content	Explanation	Requirements (general principles

			referred to in Article 5(1))
a	The name and contact details of the controller and, where applicable, the joint controller, the representative of the controller and the data protection officer;	This information serves the purpose of transparent and clear identification of the controller	Lawfulness and transparency
b	The purposes of the processing	The purposes of the processing continue with the business object of each SME. The statutes of any SME can be the tool for assessing its legitimacy. Any processing of personal data must be lawful in relation to its statutory purposes.	Lawfulness, transparency, purpose limitation
c	Description of categories of data subjects and categories of personal data	The information relates to the category of individuals whose personal data are processed, e.g. employees, customers. Examples of personal data are contact details, identification data, facial image, etc.	Lawfulness, purpose limitation, data minimization, accuracy
d	The categories of recipients to whom the personal data are to be disclosed or were disclosed, including recipients in third countries or international organizations;	Definition of 'third party' natural or legal persons, public authorities, services or bodies (Article 4(b)) 10 GDPR) that receive and process personal data. This includes natural or legal persons who, as 'processors', process personal data on behalf of the controller.	Lawfulness and transparency
e	Where applicable, transfers of personal data to a third country or international organization, including the identification of that third country or international	Such transfers are allowed on an exceptional basis even though no adequacy decision on the level of protection has been issued in accordance with Article	Lawfulness, transparency

	organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;	45(3) GDPR, and the appropriate safeguards of Article 46 are not met.	
f	Where possible, the envisaged time limits for deletion of the different categories of data;	It does not constitute optional information in the records. The time limits must be specified and the data must be deleted after the processing purpose has been fulfilled. Exceptions to time limits may be introduced on the basis of a specific legal provision for data retention, based on tax or other specific legislation pursuant to Article 17(3)(b) GDPR	Lawfulness, purpose limitation, data minimization, accuracy, storage period limitation
g	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)	The level of safety must be included and any deviations shall be specifically recorded. In case of an Impact Assessment assistance, consultation with the supervisory authority should be included.	Lawfulness, integrity and availability

B) Processor

Article 30(2)	**Content**	**Explanation**	**Requirements (general principles referred to in Article 5(1))**
a	The name and contact details of the processor or processors and of the controllers on whose behalf the processor is acting and, where applicable, the representative of the	In addition to the processor's contact details, the contact details of the controller must be included, or where they are not known to him (e.g. when several processors	Lawfulness and transparency

	controller or processor, as well as the data protection officer;	are involved) the contact details of the directly contracting controller.	
b	The categories of processing carried out on behalf of each controller	The categories of processing operations are indicated in the relevant agreement/contract between controller and processor	Lawfulness, transparency, purpose limitation
c	Where applicable, transfers of personal data to a third country or international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of the appropriate safeguards;	According to Article 49(1), such transfers are exceptionally permissible, although no adequacy decision on the level of protection has been issued in accordance with Article 45(3) GDPR, nor are the appropriate safeguards of Article 46 fulfilled.	Lawfulness, transparency
d	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)	The level of safety must be included and any deviations shall be specifically recorded. In case of an Impact Assessment assistance, consultation with the supervisory authority should be included.	Lawfulness, integrity and availability

11. How is the record kept? (printed/paper or electronic format)

The record of processing activities is kept in writing, in paper or electronic form (Article 30(3) GDPR). When compiling the file, special software programs can be used. When selecting the technical measures, the DPO may determine the appropriate requirements for each SME, taking into account: (a) effective cooperation between SME departments, (b) usefulness for SME departments and (c) availability and integrity of processed information.

12. For how long should a record be kept?

The record of processing activities must be kept up to date on the basis of the organizational needs and business activities of each SME. This information should be planned (e.g. on an annual basis) and periodically (e.g. every 3 or 6 months) depending on the activities of each company. This is because the general principle of the accuracy of personal data set out in Article 5(1)(d) GDPR covers not only the individual processing activities carried out but also the record itself, in which the information must be constantly updated, erased or rectified always for the purpose of processing.

Furthermore, the record of processing activities must be kept throughout the lifetime of each SME, as it not only facilitates the business of each company, but also serves as a tool to comply with the obligations stemming from the institutional framework for the protection of personal data. Therefore, it may be required at any time to demonstrate it to the Data Protection Authority or on this basis to meet the requirements of other supervisory authorities.

The record of processing activities does not include information on specific individuals. However, as this file combined with other structured sets or electronic records of the company can identify specific individuals (e.g. employees or suppliers), it must be kept/retained separately from the rest of the records and, where appropriate, encrypted.

5.6.2 Templates/model records of processing activities

Processing activities

A. Customer management

1. Health sector: Provision of health services
2. Education sector: Provision of education services (private schools, language schools, Greek language courses) etc.
3. Tourism - Hospitality sector: Provision of hotel and tourist services (hotel, accommodation, catering) etc.
4. Commerce sector: supply of retail trade services of products including distance e-shop services.

   The main activity of each SME for all sectors may be specified on the basis of the Business Activity Code

B. Personnel management/administration

C. Management of prospective employees

D. Management of suppliers-natural persons

E. Video surveillance

F. Direct marketing to potential customers

G. Data breach management

A. Processing activity: Customer management in the HEALTH sector

Purpose of processing	1. Provision of health/medical services [the purpose may be specified by the SME on the basis of the Business Activity Code] 2. Invoicing of services 3. Direct promotion/marketing by electronic means 4. [insert any other legitimate purposes of processing]
Type of data	1. Patient identification and billing data: name, surname, date of birth, social security number, Tax Identity Number (TIN) and tax office 2. Contact details: postal and e-mail address, telephone number (landline and mobile) 3. Payment details: credit cards – payments/debts 4. Health data: medical history, dates of visit, type of service provided, medication – treatment, insurance capacity, details of any private insurance, etc. 5. [add any other strictly necessary data if there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	Patients – customers (including minors)
Recipients	• Processors: accounting service providers, providers of IT support services, providers of hosting services, cloud providers, providers of product and service promotion services, physical security service providers [insert any other category of providers] • Financial institutions (where required) • Insurance companies (covering the insurance case) • Social security institutions and tax authorities, in accordance with the applicable insurance and tax legislation respectively • Lawyers, (if necessary) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	10 years since the last patient visit (based on the Code of Medical Ethics). Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should examine issues of tax or insurance legislation or specific legislation

General description of technical and organizational security measures	According to the list of basic personal data security measures

A. Processing activity: Customer management in the TOURISM-HOSPITALITY sector	
Purpose of processing	1) Provision of tourist and hotel services (hotel, accommodation, catering) etc. [may be specified by the SME on the basis of the Business Activity Code] 2) Invoicing of the services provided 3) Direct promotion by electronic means 4) [insert any other legitimate purposes of processing]
Type of data	1. Identification and invoicing information: name, surname, father's name, mother's name, gender, date of birth, TIN, ID number/passport 2. Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Payment details: credit cards, payments/debts 4. Reservation details: dates, type of reservation, any special preferences, etc. 5. Health data (e.g. any allergies, disabilities) and preferences (e.g. any dietary preferences), if applicable 6. [add any other strictly necessary data if there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	Customers (minors and adults)
Recipients	• Processors: accounting service providers, providers of IT support services, providers of hosting services, cloud providers, providers of product and service promotion services, physical security service providers [insert any other category of providers] • Financial institutions (where required to execute the transaction) • Tax authorities (under applicable tax legislation) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code.

	The controller should examine issues of tax or insurance legislation or specific legislation
General description of technical and organizational security measures	According to the list of basic personal data security measures

A. Processing activity: Customer management in the EDUCATION sector	
Purpose of processing	1) Provision of education services (private schools, language schools, Greek language courses) etc. [may be specified by the SME on the basis of the Business Activity Code] 2) invoicing of the service provided 3) direct promotion by electronic means 4) photo shooting of students/videos of events 5) [insert any other legitimate purposes of processing]
Type of data	1. Identification and invoicing information: name of pupil, father's name, mother's name, date of birth, gender, home address, TIN and tax office 2. Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Payment details: credit cards, payments/debts 4. Health data: information on the pupil's individual health card 5. Details of attendance and conduct: scores, absences, learning difficulties, conduct, penalties and other information included in the pupil register 6. Audio-visual material: photos, videos in the context of educational, cultural, sports or other activities of the Company (events, excursions, etc.). 7. [add any other strictly necessary data if there is a legitimate purpose and legal basis for processing]
Categories of data subjects	Customers (minors and adults)
Recipients	• Processors: accounting service providers, providers of IT support services, providers of hosting services, cloud providers, providers of product and service promotion services, physical security service providers [insert any other category of providers] [add any other category of providers, e.g. professional photographers/cameramen] • Financial institutions (where required to execute the transaction)

	• Tax authorities (under applicable tax legislation) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should examine issues of tax or specific legislation
General description of technical and organizational security measures	According to the list of basic personal data security measures

A. Processing activity: Customer management in the COMMERCE sector	
Purpose of processing	1) Supply of retail trade services of products including distance e-shop services [may be specified by the SME on the basis of the Business Activity Code] (contractual relationship) 2) Invoicing of products 3) Participation in loyalty/bonus programmes 4) Direct promotion by electronic means 5) [insert any other legitimate purposes of processing]
Type of data	1. Identification and invoicing details; name, TIN and tax office 2. Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Payment details: credit cards, payments/debts 4. Transaction details: transaction history, etc. 5. Information on participation in a loyalty/bonus program, i.e. transaction points, cash out history, etc. 6. [add any other strictly necessary data if there is a legitimate purpose and legal basis for processing]
Categories of data subjects	Customers
Recipients	• Processors: accounting service providers, providers of IT support services, providers of hosting services, cloud providers, providers of product and service promotion services,

	physical security service providers [insert any other category of providers] • Financial institutions (where required to execute the transaction) • Tax authorities (under applicable tax legislation) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should consider tax and specific legislation.
General description of technical and organizational security measures	According to the list of basic personal data security measures

A. Processing activity: Customer management in OTHER sector	
Purpose of processing	1) Provision of products/services [may be specified by the SME on the basis of the Business Activity Code] (contractual relationship) 2) Invoicing of products/services 3) Participation in loyalty/bonus programmes 4) Direct promotion by electronic means 5) [insert any other legitimate purposes of processing]
Type of data	1. Identification and invoicing details; name, TIN and tax office 2. Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Payment details: credit cards, payments/debts. 4. Transaction details: transaction history etc. 5. Information on participation in a loyalty/bonus program, i.e. transaction points, cash out history, etc. 6. [add any other strictly necessary data if there is a legitimate purpose and legal basis for processing]
Categories of data subjects	Customers
Recipients	• Processors: providers of IT support services, providers of hosting services, cloud providers,

	providers of product and service promotion services [insert any other category of providers] • Financial institutions (where required to execute the transaction) • Tax authorities (under applicable tax legislation) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should consider tax and specific legislation.
General description of technical and organizational security measures	According to the list of basic personal data security measures

B. Processing activity: Personnel management	
Purpose of processing	**1)** Execution of the employment contract **2)** Keeping a register and individual employee records **3)** Execution of payroll **4)** Promotion of the Company **5)** Employee bonuses e.g. shares **6)** [insert any other legitimate purposes of processing]
Type of data	1. Identification: name, surname, father's name and mother's name, ID number, TIN and tax office, social security number, gender, nationality, date and place of birth 2. Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Employees' personal, family and employment situation and data of dependents: name and date of birth (where required) 4. Data on professional skills and qualifications, and career development in the Company: curriculum vitae, copies of diplomas, information on work experience, professional certifications, professional

	licenses, registration number in professional registers, certificate of fulfilment of military obligations, letters of recommendation and certificates of work experience by previous employers, assessments, productivity bonuses, promotions, training, educational licenses, criminal record (where required), date of commencement of employment. 5. Data concerning your health (where applicable). 6. Social security data: notification to the insurance body (EFKA), notice of recruitment to the Manpower Employment Organization (OAED) (where required), retirements, copies of certificates relating to compulsory insurance 7. Bank account (Bank and IBAN) for crediting fees 8. Computer network access data, the Company's databases, as well as on the Internet from fixed and/or portable electronic devices of the Company (e.g. laptops, mobile phones, tablets), and/or the data stored therein (based on the Company's policy/regulation on the use of its electronic means) 9. Photographs and videos with audiovisual material (in the context of social events and/or promotional actions of the Company). 10. [add any other strictly necessary data if there is a legitimate purpose and legal basis for processing]
Categories of data subjects	Employees (employees with any employment relationship or work or independent service contract)
Recipients	• Processors: accounting service providers, providers of IT support services, providers of hosting services, cloud providers, physical security service providers, [insert any other category of providers] • Financial institutions (where required to execute the transaction) • Tax authorities (under applicable tax legislation) social security institutions, health institutions (where applicable) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable)

	• Co-operating insurance companies (e.g. group insurance policy) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should examine tax and specific legislation issues
General description of technical and organizational security measures	According to the list of basic personal data security measures

C. Processing activity: Management of prospective employees	
Purpose of processing	Information on the possibility of employment in different jobs within the SME and on the assessment of the fulfilment of recruitment conditions for a specific job [insert any other legitimate purposes of processing]
Type of data	7. Identification details, full name, father's name and mother's name, ID number, gender, date and place of birth, nationality. 8. Contact details, postal and e-mail address, telephone number (landline, mobile). 9. Curriculum vitae, marital status, any disability. 10. Training and background data, professional experience. 11. Ground for rejection of a request for recruitment. 12. [add any other strictly necessary data if there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	prospective employees
Recipients	• Processors: providers of IT support services providers of hosting services, cloud providers [insert any other category of providers] • Lawyers (if required), • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	For unsuccessful candidates: retention for a period of 6 months and after being informed of the possibility of employment in another job within the SME, data retention for 1 or 2 years, respectively, on the basis of consent.

General description of technical and organizational security measures	According to the list of basic personal data security measures

D. Processing activity: Management of suppliers-natural persons	
Purpose of processing	1. Supply of products/services 2. Fulfilment of tax obligations 3. [insert any other legitimate purposes of processing]
Type of data	1.Identification data, name, TIN 2.Contact details: postal and e-mail address, telephone number (landline, mobile) 3. Transaction history (payments, debts, etc.) 4. [add any other strictly necessary data where there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	Suppliers-natural persons
Recipients	• Processors: accounting service providers providers of IT support services providers of hosting services, cloud providers physical security service providers [insert any other category of providers] • Financial institutions (where required to execute the transaction) • Tax authorities (under applicable tax legislation) • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should consider issues of tax and specific legislation
General description of technical and organizational security measures	According to the list of basic personal data security measures

E. Processing activity: Video surveillance

Purpose of processing	Protection of persons and property
Type of data	Image data of natural persons
Categories of data subjects	Employees, customers and SME visitors
Recipients	1) Competent judicial, prosecutor and police authorities (where required) 2) The victim or perpetrator of a crime
Data retention time	15 days (exceptionally, 30 days for a specific incident or 3 months if it concerns a third party). For apartments (e.g. clinic, private tutorial school): 48 hours
General description of technical and organizational security measures	According to the list of basic personal data security measures

F. Processing activity: Potential customer outreach	
Purpose of processing	1. Promotion of products and services by electronic means (email, SMS) 2. e-Newsletters 3. [insert any other legitimate purposes of processing]
Type of data	1. Identification of a natural person: name and surname 2. Contact details: mobile phone, email 3. [add any other strictly necessary data where there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	Potential customers
Recipients	• Processors: a marketing service provider on behalf of the SME, providers of IT support services providers of hosting services, cloud providers [insert any other category of providers] • Lawyers (if required) • Bailiffs, notaries, judicial, prosecutor and police authorities, as well as supervisory authorities (where applicable) • [insert any other category of legal recipients]
Data retention time	Until the withdrawal of consent or the activation of the right to object

General description of technical and organizational security measures	According to the list of basic personal data security measures

G. Processing activity: Handling of a personal data breach incident	
Purpose of processing	Investigation of the incident of breach and information of subjects affected by the incident and registration of the incident in the internal register/record of the company
Type of data	1. Identification and contact details of an affected natural person: name, address, telephone, email. 2. Information on the nature of the breach 3. [add any other strictly necessary data where there is a legitimate purpose and a legal basis for processing]
Categories of data subjects	Customers, employees, suppliers
Recipients	1. The processor contracted by the company for the investigation of the data breach 2. Bailiffs, notaries, judicial, prosecutor and police authorities, supervisory authorities (where applicable) 3. [insert any other category of legal recipients]
Data retention time	Maximum 20 years for limitation of civil claims against the controller under Article 937 Civil Code. The controller should address issues of specific legislation
General description of technical and organizational security measures	According to the list of basic personal data security measures

5.7 Security measures

5.7.1 List of basic organizational and technical security measures for the SMEs

1. Introduction

The GDPR does not contain specific security measures that controllers and processors have to apply. A risk-based approach shall be taken to determine the appropriate safety measures. Controllers and processors must take particular account of these measures and apply them where appropriate. These measures are also closely linked to the obligation of controllers to take appropriate technical and organizational data protection measures by design and by default. In any case, implemented measures must be reviewed periodically at least. It is stressed that sector-specific legislation on the processing of personal data, although the logic of identifying risk-based security measures generally follows, lays down specific minimum security measures.

2. Organisational security measures

1. Security policy

The controller must draw up a written security policy.

Security Policy is a document describing the security objectives and procedures to be followed in order to achieve these objectives. It determines the commitment of the Administration and the approach of an organisation or business to the security of information systems and networks and the protection of personal data held by the controller.

The security policy may be either uniform in order to cover all information systems and procedures related to the processing of personal data, or consist of sections where each refers to a sub-system for the processing of personal data or a sub-sector of security (such as an individual policy on the management of backups, for managing security breach incidents, etc.). In the latter case, individual policies are annexes to and mentioned in the general security policy. It must also be free from specialised technical conditions and references, which may make its application difficult and make it dependent on specific technological choices.

If part or all of the processing takes place exclusively on systems under the sole supervision of the processor, then this should be indicated in the security policy. The part of the security policy relating to the processor should also be notified to the processor. In such a case, this part of the security policy should explicitly mention the processor's obligation to fully adopt and implement it.

2. Training and awareness-raising of staff

The controller must train its staff in matters of personal data protection, as well as in specific security-related IT system functions (e.g. use of unpredictable passwords and passwords, how to detect and report security breaches, correct use of e-mails and detachable storage media).
The training on recruitment should include as a minimum notification to security policy employees, which should as far as possible be ascertained to be fully understood by all, as well as of data breach and disaster recovery management procedures, insofar as they fall within their remit. It would be advisable to have a corporate website (intranet) where a description of the basic security procedures that staff members need to know is posted. Training should also continue after recruitment, either in significant changes in security procedures or when important safety issues arise. In addition, more specific information forms should be drawn up with regard to the purpose of education.

3. Management of roles and responsibilities

Organisational roles should be created for specific tasks within the organisation/company and staff should be linked to their respective roles. There must be a clear separation and assignment of tasks/responsibilities to each employee, based on their role. Roles must be formally assigned (in writing). Staff members should have the right of access only to the strictly necessary personal data, on the basis of the responsibilities and tasks assigned to them and dictated by their role (in other words, each member of the organisation is given specific access rights in accordance with the roles they receive).
There must be a procedure for the periodic review and review of authorisations and access rights for all stages of the staff's career (recruitment, transfer, change of duties, leaving, etc.).

Confidentiality commitment
The controller should select persons with equivalent professional qualifications that provide sufficient guarantees in terms of technical knowledge and personal integrity for confidentiality. To this end, it is necessary to take specific measures to bind staff processing personal data to confidentiality, in particular where such staff are not already bound by confidentiality. The drafting of professional normative texts can also help in this direction.

4. Managing processors

Where the controller entrusts the processing of data to a processor, the delegation shall be made in writing, unless the delegation is provided for in law. The delegation must ensure that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met. Written contracts must also contain the levels of service to be achieved by the processor (in terms of security and data quality).
The processor must take appropriate organisational and technical measures to ensure the safe keeping and processing of the controller's personal data. The controller must ensure that the processor respects the terms of the controller's security policy insofar as it concerns the processor with regard to rules on access to systems, management of security incidents, physical security measures, etc. Access rights to members of the processor's staff in the controller's systems shall be granted only when this is necessary for the implementation of their contractual obligations. The minimum necessary empowerments should be conferred, which in turn should be abolished upon termination of the contractual obligation.
Employees of the processor who, during the contract period, process personal data on behalf of the controller must be bound in writing by an appropriate confidentiality statement.

5. Destruction of data

Prior to the destruction of paper or electronic files containing personal data, appropriate measures must be taken to ensure the complete and permanent deletion of such data. In particular, as a minimum, the Authority's Directive 1/2005 on the safe destruction of personal data at the end of the period required for carrying out the purpose of the processing should be followed. The controller must have a specific written procedure for the destruction of the data, both when it comes to a planned mass destruction of data, and when it comes to the destruction of data on a daily basis (e.g. using document destroyers) and inform its employees accordingly.

6. Document display

Files containing personal data (physical file) must be placed in containers and not exposed to public view. The transfer of physical files to different offices or organisational units should be recorded. Documents and portable storage media in offices should not be left unsupervised. Other devices that may be used for interception or for displaying personal data in plain sight, such as copiers, fax machines, printers, etc. should be properly protected.

7. Handling of personal data breach incidents

The controller must have procedures in place for identification, reporting, notification (as set out in Art. 33 and 34 GDPR) and immediate response to personal data security breaches in the context of the processing system used. These procedures should first include the actions necessary to investigate the incident – how to report an incident, staff to be activated, files-systems to be investigated, what the incident management file will contain, etc. There should be a record of each incident in a relevant record, including the time it took place, the person

who reported it and to whom it was reported, an assessment of the consequences and relevance of the incident, the recovery/correction procedures followed, a procedure for notifying the Authority as well as a possible procedure for informing affected persons (data subjects) depending on the extent of the incident and the consequences thereof for the natural persons concerned.

8. Control procedures

There must be procedures for the preparation of planned audits (either internal or external, on an annual basis) to reflect and monitor compliance with security measures and their effectiveness. The result of the checks may be to modify some security measures or to add new ones. The results of the checks accompanied by the necessary amendments to the security measures must be submitted to the security officer and the controller must be informed. The Security Officer should make use of this finding by making the necessary amendments to the security measures as well as to the Security Policy.

3. Technical Security Measures

1. Data protection techniques

The processing (transmission, storage, etc.) of personal data should consider the use of the following data protection techniques based on the risk posed by the processing to the rights and freedoms of data subjects.

Encryption

This is a process of transforming personal data into an incomprehensible form using an encryption algorithm and a secret key, which is reversed through the reverse process of decryption using the key. The security of personal data is based on the use of known secure encryption algorithms as well as the size and secrecy of the key. Personal data are generally processed after decryption.

Encryption can be used to protect data stored in databases, computers and storage devices (e.g. USB flash drives) as well as during transmission via networks (e.g. Internet, e-commerce), mobile phones, wireless communication systems, Bluetooth devices and bank cash machines.

Pseudonymisation

It is defined as the processing of personal data in such a way that the data can no longer be attributed to a particular data subject without the use of supplementary information, provided that such supplementary information is kept separately and subject to technical and organisational measures to ensure that it cannot be attributed to an identified or identifiable natural person. This involves replacing one or more identifiers of data subjects with aliases and protecting and separating supplementary information (i.e. matching identifiers/identifiers with pseudonyms) by pseudonymised data.

In determining whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as its separation, either by the controller or by a third party for the direct or indirect identification of the natural person. In determining whether any means are reasonably likely to be used to identify the natural person, all objective factors, such as the costs and time required for identification, should be taken into account, taking into account the technology available at the time of processing and technological developments.

Unlike anonymisation, this is a reversible technique. It includes techniques such as data masking (covering part of the data with random characters or other data), scrambling, tokenisation (replacement of critical personal data with a randomised number of the same length and format called “token”) and blurring. Among the techniques that can be used to produce pseudonyms are cryptographic algorithms. The matching of “identifiers” with “pseudonyms” is ensured by the secrecy of the key combined with the strength of the algorithm. The original identifier can be retrieved from the alias by decryption.

The use of pseudonymisation can reduce the risks for data subjects and make it easier for controllers and processors to comply with their data protection obligations. Depending on the risks involved, the appropriate pseudonymisation technique may be chosen each time and possibly combined with anonymisation techniques.

Anonymisation

It is defined as the process of deleting personal identifiers in records of stored data, so that it is no longer possible to relate these data to the data subject to whom they relate. This is an irreversible removal of sufficient data so that the identity of the data subject can no longer be verified.
The technique of anonymisation differs from that of pseudonymisation because it makes it impossible to identify the data subject, contrary to the technique of pseudonymisation which does not delete the identity, but is replaced in such a way that additional information is required to enable the identification of the original subjects. Therefore, also on the basis of recital (26), the GDPR does not apply anonymised data as they cannot be associated with an identified or identifiable natural person.

2. Backups

The controller must develop a specific policy for receiving and managing backups. The policy must include at least the rules/procedures relating to: the selection of critical resources (applications, operating systems, files, user file data, etc.) that need to be backed up, the frequency of backup creation/receiving (regularly, on a daily or weekly basis, depending on the size and type of data, as well as when the data are changed), their appropriate marking, their secure storage and the correct recovery of the data from the backups (including the periodic integrity/reliability check of the copies received). This should ensure that in the event of security emergencies and data loss or destruction for other reasons (e.g. material failure), their availability and integrity remains.

A backup must be kept in a different space/physical location from the primary data, with security measures depending on the measures adopted for the primary data. Measures must also be taken to ensure safe transport.

3. Management of user accounts and passwords

The controller must adopt specific procedures for the management of user accounts, which must include as a minimum procedures for adding, modifying attributes and deleting an account. A different access account must be assigned to each user.

Mechanisms should be developed to prevent access to resources/applications/files by unauthorised users: in essence, appropriate measures must be in place to ensure that users are properly identified and authenticated, taking into account existing multi-factor authentication methods and making use of them where necessary,

while at the same time a specific allocation of rights/authorisations to each user should be made at technical level.

The controller must adopt a specific user password management policy, including at least acceptance rules for the minimum length and permissible characters of the passwords (complexity of passwords), the history of the password and the frequency of change.

Passwords must not be recorded somewhere in their actual form (either in a physical or electronic file). If passwords are kept electronically as part of the user identification-authentication process, they must be in an unreadable form from which it should not be possible to retrieve their original form. Users should also be obliged to change the (default) password assigned to them from the outset, as well as being obliged to change their password at regular intervals.

4. Management of mobile or portable devices

There must be procedures for effective encryption (selection of modern and powerful encryption algorithms, appropriate key size and techniques for managing them, etc.) files with personal data held on portable storage media (e.g. USB disks, etc.), since for these cases the risk of data leakage increases.

5. Safety of workstations

Protection against malware

There must be malware protection for all computers (both employees' personal computers and servers) that hold or process personal data. This can be achieved (in addition to the proper use of these by employees) with antivirus programs, as well as by using firewall programs. Both antivirus and firewall must have the latest updates at all times. In addition, security updates must be installed on the computer operating system (if they are connected to the Internet) at regular intervals.

Security Updates

Provision must be made regarding the immediate installation of all proposed security updates of the programs/operational system/databases of the workstations/servers.

Rights to manage programmes/applications

Simple user actions should not be allowed on computers that affect their overall configuration (e.g. disable virus detection programs, install new programs or change existing settings, etc.). A periodic check of the installed software should be carried out to identify any programs installed outside the approved procedures.

Management of detachable means

Computers used by end-users must not be able to extract data using detachable means (e.g. USB, CD/DVD) – unless approved by the Security Officer (or other type of authorisation, through a security policy procedure).

6. Communications security

Firewall

The controller and/or processor must ensure that connections to their network are allowed only through the firewall and apply rules on incoming and outbound traffic control. They must also record all successful authorised connections and all rejected attempts to connect to an event log, in order to detect attempts to breach the security of its infrastructure, in order to appropriately strengthen the rules to prevent them.

Remote Access (VPN)

All remote employee connections to the controller's network terminals must be made through a secure communication channel with appropriate end-to-end encryption (virtual private networks) in order to reduce the risk of unauthorised third-party access to such data transmission.

4. Physical Security Measures

1. Physical access control

Appropriate physical access control measures must be in place in the critical areas where the physical equipment (including telecommunications and network wiring) supporting the information systems and the processing of personal data is located, so that only authorised personnel can have access to (for example, some sites – such as those found on network equipment – must be permanently locked). In some cases (depending on the nature of the data and the risks involved) it may be appropriate to record any access to a specific physical area.

2. Protection against natural disasters

Appropriate measures must be taken to protect buildings, critical spaces, computer room, staff offices, IT equipment and the physical record-keeping area against damage caused by natural disasters or malicious actions such as flooding, overheating, fire, earthquake, explosion, water leakage, power failure, burglary/theft, vandalism, etc. Indicative measures in this direction are: alarm, security doors and windows, fire protection, removal of equipment from water pipes and dust sources, humidity and flood detectors, uninterrupted power supply through stabilisers/generators, etc.

5.8 Data Breach handling

5.8.1 Information and procedures to the SME how to identify and handle personal data breaches

1. What is a personal data breach

1.1. Definition

A personal data breach is defined as a breach of security leading to destruction, loss, alteration, unauthorised disclosure or access to personal data (Article 4(12) GDPR). The breach of security, which affects personal data, may occur either accidentally or unlawfully.

✓ ***Any personal data breach is a security incident related to and having an impact on personal data.***

Examples of breaches that may affect an SME are given in section 5.

1.2. Types of data breach

A personal data breach may result in a breach of confidentiality (secrecy), the integrity and availability of personal data as well as any combination of them. In particular:

- The breach of **confidentiality occurs** when personal data are disclosed to unauthorised persons.
- The breach of **integrity** occurs when there is alteration of personal data.
- The breach of **availability** occurs when personal data ceases to be available to authorized users whenever their use is required — there is a loss of access or destruction of personal data.

2. Obligations to detect, manage and address the breach

2.1. Data breach management procedures

The SME, as the controller, must implement appropriate technical and organizational measures with the main objective of preventing a breach of personal data; in the event that such an incident does take place, it shall be detected and addressed in a timely manner.

For this purpose, the controller must be prepared before the breach takes place and must have designed and prepared a management and response plan. This plan should set out internal procedures for the following:

- ✓ the early detection of security incidents (control of log files, security checks and vulnerabilities, use of firewalls, reports by employees, etc.)
- ✓ the immediate reporting of any security incident and all relevant information to the relevant person or group of persons designated by the SME — informing the DPO and the security officer if they have been designated;
- ✓ the timely analysis and investigation of any security incident to establish with a reasonable degree of certainty that a breach has occurred, resulting in the personal data being compromised;
- ✓ an assessment of the risk arising from the breach (negligible risk, risk or high risk) and any adverse effects of the breach on the rights and freedoms of the affected persons;
- ✓ taking and documenting the decision to submit a notification to the supervisory authority and possibly to inform affected persons (see section 3) on the basis of the level of risk;
- ✓ as soon as the controller becomes aware of the breach, it shall take corrective measures to limit and address it, mitigate any adverse effects on individuals and prevent further breaches in the future;
- ✓ recording and documenting the breach in an internal register as it evolves.

✓ ***Employees must be informed of the above procedures and know what to do in the event of a breach.***

2.2. Possible consequences of the breach and assessment of the level of risk

A breach may potentially have several significant adverse effects on individuals, which can lead to physical, material or non-material harm. Such harm may include loss of control over their data, restriction of their rights, discrimination, identity theft or fraud, financial loss, unlawful reversal of pseudonymisation, damage to reputation and loss of confidentiality of data which are protected by professional secrecy. It may also include any other significant economic or social disadvantage for such persons.

The controller should assess the risk of adverse consequences for individuals as a result of a personal data breach. This will allow the controller to (a) take effective actions to limit and address the breach knowing the

seriousness of its consequences and (b) fulfil the obligations of the GDPR vis-à-vis the supervisory authority and affected persons based on the level of risk.

The GDPR distinguishes three levels of risk on the basis of an objective assessment resulting from the specific circumstances of the breach including the severity of the impact and the likelihood that it will occur:

- ✓ **Negligible risk probability**: when all three security parameters are met: confidentiality, integrity and availability
- ✓ **Risk**: exists where the breach is likely to lead to physical, material or non-material harm to the affected persons;
- ✓ **High risk**: exists where particularly serious harm to affected persons is likely to occur as a result of the breach

Factors taken into account in the risk assessment:

- ✓ the type of breach
- ✓ the nature, sensitivity and volume of personal data (e.g. health data, identity documents, financial data, credit card details)
- ✓ whether the identification of persons is easy
- ✓ the seriousness of the consequences for persons (e.g. identity theft, physical injury, psychological suffering, humiliation)
- ✓ the specific characteristics of the person (e.g. children, vulnerable persons, etc.)
- ✓ the specific characteristics of the controller (e.g. object of activities)
- ✓ the number of persons affected

3. Controllers' obligations under the GDPR

The obligations of controllers with regard to the personal data breach under Articles 33-34 GDPR are set out below.

SME obligations under the GDPR:

- ✓ Notification of the breach to the Authority, unless it is unlikely to result in a **risk, without delay or at the latest within 72 hours**
- ✓ Notification of the breach to affected persons in addition to the notification to the Authority where the breach is likely to result in a **high risk, i.e. in less than 72 hours without delay.**
- ✓ Recording and documenting any breach in an internal register irrespective of the level of risk on which the above two obligations are based.

Each of those obligations is analysed further below.

3.1. Notification to the Authority

A. When is required

If an incident of breach is detected, the controller must immediately assess its seriousness and its consequences and adverse effects on individuals (data subjects).

If the breach is likely to create a **risk** leading to adverse effects on the rights and freedoms of natural persons, a notification shall be submitted to the Authority[97] without undue delay and no later than 72 hours after its detection. A gradual notification shall be permitted without undue delay where further investigation is necessary, in particular in complex incidents, and the controller shall duly justify the delay.

B. When it is not required

Notification is mandatory unless the breach is unlikely to cause a risk. For example, no notification is required in case of data loss if there is certainty that the data has been properly encrypted using a modern and robust algorithm, in accordance with international standards, provided that the encryption key remains unaffected in the secure possession of authorised users and there is a recent complete and unaltered backup.

C. What information does it include

The minimum required elements of the notification of a breach event are the following:

- the identity and contact details of the controller;
- the name and position of a person responsible for contacting the Authority;
- information on the timing of the incident (if the incident is in progress, start and end time, time and manner that the controller received knowledge of the incident, time of notification from the processor),
- information on the nature of the incident
    - type of breach (confidentiality, integrity, availability or any combination of them)
    - nature of the incident (e.g. device loss, security attack, accidental data communication, etc.)
    - cause(s) of the incident (e.g. human error, malicious action, etc.),
- type of data related to the incident
    - simple data (identification data, access details to system, TIN number, Social Security number, ID number, contact details, financial details, location details, etc.)
    - specific data (racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, health data, sexual life or sexual orientation data);
- persons concerned by the incident
    - number of files and persons
    - categories of subjects (working students, minors, customers, subscribers, service users, etc.),
- measures taken before the incident
- consequences of the incident
    - type of breach,
    - physical, material or non-material damage or significant consequences for persons
- actions after the breach
    - inform the persons affected by the incident
    - measures to address the incident
    - cross-border incidents (breach cases affecting persons in more than one Member State and submitted to the lead supervisory authority or other affected Member States).

[97] Information for submitting a notification to the Authority is available via its website at https://www.dpa.gr/index.php/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis/upovoli_gnwstopoihshs_paraviashs.

3.2. Communication of the data breach to affected data subjects

A. When is required

Where the breach is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall have an obligation to notify the affected persons of the breach as soon as possible and without undue delay.

Such information shall be timely, explain to the persons concerned clearly what has happened and contain recommendations and proposed measures to be taken by such persons. In this way, affected persons have the possibility to act immediately and to protect themselves by taking appropriate measures to mitigate any adverse effects of the breach.

B. When it is not required

There is no need to notify affected persons if the three conditions referred to in Article 34(3) GDPR are fulfilled, namely:

- The controller implemented appropriate technical and organisational measures to the affected data prior to the breach, notably measures that render the data unintelligible to unauthorised persons such as state-of-the-art encryption (see example of section 3.1 for no notification requirement).
- The controller has taken measures immediately after the breach to ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
- Communication with affected persons involves disproportionate efforts, in particular if the contact details have been lost as a result of the breach or were not known from the outset. In such a case, the controller shall make a public announcement or take a similar measure by which persons are informed in an equally effective manner.

✓ ***The decision not to communicate the breach to the affected persons shall be duly substantiated*.**

C. What information does it include

Communication to natural persons should be made in the most appropriate and effective manner, in the form of personalised information and not by means of a general communication, to the extent possible.

✓ The information to the affected persons essentially includes the same information as that provided to the supervisory authority in the context of the notification (see Section 2.1C).
✓ Emphasis should be placed on recommendations to the natural persons concerned to mitigate potential adverse effects.

3.3. Documenting and substantiating the breach

A. When is required

The controller has an obligation to internally record and substantiate any incident of breach regardless of the level of risk (Article 33(5) GDPR).

✓ Any breach shall be included in the internal register of the SME, whether or not a notification is required.

✓ The internal register shall be used, inter alia, to demonstrate compliance in any audit by the supervisory authority.

B. What information does it include

While it is up to the controller to determine the method and structure to use when documenting a breach, there are some key elements that should be included in each case with regard to the information to be recorded.

The controller must record the causes of the breach, what happened, the data affected, the consequences of the breach as well as corrective actions taken.

In addition to these details of the breach, it is recommended to also record the rationale of its decisions to address a breach. More specifically, if a breach is not disclosed, a reasoned justification for this decision should be recorded. This justification should include the reasons why the controller considers that the breach is not likely to result in a risk to the rights and freedoms of persons. Alternatively, if the controller considers that any of the conditions that do not require communication to natural persons are met (see section 3.2B), it should be able to provide appropriate evidence.

✓ The internal register records essentially the same information as that provided to the supervisory authority in the context of the notification (see section 2.1C) ✓ Evidence of compliance (e.g. risk assessments that led to the decision not to disclose the incident or to communicate it to affected persons) should also be recorded. ✓ If personal data are recorded, the controller must specify a retention period and a lawful basis for processing.

4. Obligations of processors under GDPR

If the processor becomes aware of a data breach processed on behalf of the controller, he/she must inform the controller without delay and in less than 72 hours. The obligation of the processor to inform allows the controller to remedy the breach and to decide whether to submit a notification and inform the affected persons. The obligations of the controller start from the moment of notification by the processor.

✓ Details of the controller's and processor's responsibilities in the event of a breach should be explicitly stated in the contract by which the processing is delegated.

5. Examples of breaches that may affect a small and medium-sized enterprise

The following examples are taken from European Data Protection Board Guidelines 1/2021.

Category 1: ransomware attacks

This is a category of attacks where personal data are encrypted by malware and the attacker asks for a ransom in order to decrypt it. Without decryption, the data cannot be processed and is no longer available to the controller. Malicious action is usually limited to encryption without extracting or altering the data, in which case it is usually a breach of availability.

Obligations	Description of the data breach
1st incident: Notification to the Authority: NO Information to persons: NO Recording and documentation: YES	**Type of company**: small construction company **Type of data and categories of subjects**: personal data of dozens of customers and employees stored in the company's system **Type of attack:** the attacker attempted to encrypt the data, which were already encrypted by the SME, and they did not enter into his possession (without exfiltration) nor were they tampered/altered **Type of breach**: lack of availability of data for a few hours (until retrieved from backup) **Response measures:** retrieval of data from (inaccessible from attack) backup within a few hours **Consequences for data subjects**: none because the data was retrieved from the backup and did not come into the possession of the attacker
2nd incident Notification to the Authority: YES Information to persons: NO Recording and documentation: YES	**Type of company**: company in the agricultural sector **Type of data and categories of subjects**: simple personal data of a few dozen customers and employees stored in a computer of the company **Type of attack:** encryption of data without extraction (without being in the possession of the attacker) and without falsification/alteration **Type of breach**: lack of availability for five days **Response measures:** entry of data into the system from the physical file in the absence of a backup in electronic format, lasting five days **Consequences for data subjects**: minor delays in delivering orders to customers
3° Incident: Notification to the Authority: YES Information to persons: YES Recording and documentation: YES	**Type of company**: hospital **Type of data and categories of subjects**: personal data of tens of thousands of employees and patients of the hospital's IT system **Type of attack:** encryption of the data by the attacker without data extraction and without tampering/alteration **Type of breach:** lack of availability for two days

	Response measures: retrieval of most of the data within two days of the backup available and unaffected by the attack in electronic format. **Consequences for data subjects:** significant consequences such as cancellations and postponements of surgery, delays in the provision of health services

Category 2: data exfiltration attacks

This is a category of attacks in which the attacker extracts personal data.

Obligations	**Description of the data breach**
1st incident: Notification to the Authority: YES Information to persons: YES Recording and documentation: YES	**Type of company**: employment office **Categories of data and subjects**: simple personal data of 213 applications submitted via a web application and stored on the webserver **Type of attack:** installation of malicious code on the website resulting in unauthorised persons gaining access to online applications **Type of breach**: breach of confidentiality and possibly integrity if data changes are made **Response measures:** restoring data to pre-infringement status, correcting vulnerability and implementing new security measures to avoid such breaches (such as record integrity checks, keeping daily data inputs into the web application, periodic security checks as well as penetration assessments and tests) **Consequences for data subjects**: access of the attacker to important data contained in job applications, which can be exploited in various ways (sending unsolicited communication, identity theft, etc.).
2nd Incident: Notification to the Authority: NO Information to persons: NO Internal documentation: YES	**Type of company**: cooking website **Type of data and categories of subjects**: the unintelligible hashes of the 1200 users' passwords. The database shall store the result of a strong hash function using a "secret key" for each password. Users only use aliases as usernames and are discouraged to use e-mail addresses for this purpose **Type of attack:** use of SQL injection vulnerabilities resulting in unauthorised persons gaining access to the database with users' passwords **Type of breach**: breach of confidentiality

	Response measures: correcting vulnerability, using strong encryption, limiting the number of failed login attempts, carrying out security checks, using authentication methods that prevent the need to process passwords from the server. **Consequences for data subjects**: there were no consequences due to the use of a strong method of converting passwords into irreversible and incomprehensible form; as a rule, no contact details of users were exposed

5.8.2 Employee awareness leaflet on personal data breaches

1. What is a personal data breach

An incident of a personal data breach occurs when the personal data for which the SME is responsible, such as details of customers, potential customers, employees, prospective employees, suppliers (who are natural persons) are disclosed, accidentally or unlawfully, to unauthorised persons, or become, temporarily or permanently, unavailable or altered.

Key elements of the personal data breach are the following:

- ✓ security breach leading to destruction, loss, alteration, unauthorised disclosure or access to personal data (Article 4(12) GDPR);
- ✓ the breach of security has an impact on the personal data and may occur either accidentally or unlawfully;
- ✓ such a breach may have an adverse effect on the rights and freedoms of natural persons;
- ✓ the breach entails obligations of SMEs under the GDPR vis-à-vis the supervisory authority and affected persons depending on the level of risk.

2. What are the types of personal data breach

- ✓ Confidentiality breach: it takes place when personal data are disclosed to unauthorised persons.
- ✓ Breach of integrity: it occurs when personal data is tampered with or falsified.
- ✓ Breach of availability: it occurs when personal data ceases to be available to authorised users whenever their use is required — there is a loss of access or destruction of personal data.

3. What are the possible effects of a data breach incident on individuals

A breach may potentially have several significant adverse effects on individuals, which can lead to physical, material or moral harm. Such harm may include loss of control over their data, restriction of their rights, discrimination, identity theft or fraud, financial loss, unlawful removal of pseudonymisation, damage to reputation and loss of confidentiality of data which are protected by professional secrecy. It may also include any other significant economic or social disadvantage for such persons.

4. What are the main obligations of my Company in the event that a personal data breach occurs

- ✓ As soon as it becomes aware of the breach, the SME must immediately assess its seriousness and its consequences and adverse effects on natural persons.

- ✓ The SME must take immediate action to address and reduce the breach as well as measures to correct the problem and avoid such breaches in the future.

- ✓ **Obligation to notify the Authority:** If the incident of breach **endangers** the rights and freedoms of natural persons, the SME must submit a notification to the Authority immediately or no later than 72 hours after it becomes aware of the incident.

- ✓ **Obligation to inform affected persons:** If the incident of breach poses a **high risk** to the rights and freedoms of natural persons, the SME must in addition to the notification inform the affected persons in an appropriate and comprehensible manner without delay (i.e. in less than 72 hours).

- ✓ **Obligation to keep an internal register:** In any case, the SME must record and document any incident, regardless of the level of risk, in an internal register.

5. What are typical examples of breaches that may affect my Company

- ✓ Send an email with customer personal data to the wrong recipient.
- ✓ Hardware failure and shutdown of the information system.
- ✓ Theft of the backup of the database.
- ✓ Theft of documents with personal data from an office or unlocked locker.
- ✓ Theft or loss of a laptop/device (e.g. USB stick) with personal data.
- ✓ Malware infection resulting in the unlawful transfer of personal data files to third parties.
- ✓ Accidental deletion of personal data from the database.
- ✓ Export data from a website with SQL Injection attack.
- ✓ Deception of an employee resulting in the communication of personal data to malicious persons.

6. How can I detect a possible data breach incident

An incident of a personal data breach relates to the personal data collected and processed by the SME to carry out its activities. The incident will therefore concern the data of a category of natural persons such as customers, potential customers, employees, prospective employees, suppliers-natural persons or other categories.

The incident of a breach affects the security of personal data such as destruction or loss of data, disclosure of such data or access to it by unauthorised persons or alteration of the data.

Since any personal data breach incident is a security incident affecting personal data, it is advisable for the employee to inform the relevant SME persons of any security issue without being clearly linked to personal data such as if he/she finds infection of his/her computer or mobile device by virus software, unlawful installation of programs or applications, malfunction of his/her computer, etc.

7. What actions can I proceed to if I notice a possible data breach incident

- ✓ Immediately inform the competent persons of the Company of the possible incident of breach, in accordance with the respective policy, and/or the Data Protection Officer, if he/she has been designated. In any case, the IT Officer or the IT Department may be informed.

- ✓ Temporarily discontinue any processing of personal data affected by the breach incident.

- ✓ Gather, if possible, any evidence related to it without altering or destroying them.

- ✓ Assist the persons responsible in investigating the incident with information that I may know about it or about the characteristics and means of processing the data concerned.

8. What steps can I take to protect the data I handle from a possible data breach incident

- ✓ Do not leave documents in your office and the lockers you have access to.
- ✓ Check the addresses of the recipients of the emails.
- ✓ Do not store personal data on mobile devices without encryption.
- ✓ Do not store data on your personal computer at the end of the teleworking unless it is encrypted.
- ✓ Learn and implement your company's policies.
- ✓ Keep the data you handle with confidentiality.
- ✓ Choose an appropriate password, do not disclose it to others and change it on a regular basis.

5.9 Assignment of data processing to contractors/processors

5.9.1 Frequently Asked Questions for processors

1. I use accounting services-office/cloud services/computer services for the company's information system/. Are these service providers processors?

To the extent that the controller-company entrusts such service providers with a specific activity and defines the purpose and means by which the aforementioned activity will be carried out on its behalf, the providers of such services are processors and the relevant contract should be concluded.

2. When in the context of a contractual relationship the processor can be considered as a controller?

In the contractual relationship of a controller — processor, the processor infringes the GDPR by not applying the controller's instructions for the processing of personal data in accordance with the work assigned to it and specifying the purposes and means of the processing itself. In this case, this processor will be considered as a controller in relation to the specific processing assigned to it and will be subject to penalties for non-implementation of the instructions of the controller.

3. What are the processing security measures to be taken by the processor?

Article 32 GDPR states that, taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure an appropriate level of security against risks. The Controller shall assess the risks posed by the processing to the rights and freedoms of natural persons and shall take measures to mitigate those risks. Depending on the significance of the risks, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis;

c. the ability to restore the availability and access to personal data in due time in the event of a physical or technical incident;

d. Procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

A list of basic security measures is available here.

4. For which specific rights should the processor assist the controller?

The processor shall assist the controller in fulfilling the following rights:

a. informing the data subject when personal data are collected from the data subject

b. informing the data subject where the personal data have not been collected by the data subject

c. access by the data subject

d. correction

e. erasure ("right to be forgotten")

f. restriction of processing

g. obligation to notify concerning rectification or erasure of personal data or restriction of processing

h. data portability

i. objection

j. right of the data subject not to be subject to a decision taken solely on the basis of automated processing, including profiling.

General information on the exercise of data subjects' rights is available here.

5. What are the obligations of the processor?

The processor's obligations are:

- To create and maintain a record of activities for each controller with whom it contracts;
- To implement the instructions of each controller and not carry out any further processing of data beyond its express instructions;
- To implement technical and organisational measures to ensure the processing entrusted to it;
- To assist the controller, where provided for in the relevant contract:
  i. In managing requests for the exercise of data subjects' rights;
  ii. in cases of infringement
  iii. in carrying out an impact assessment study, if necessary
- To appoint a Data Protection Officer, if applicable
- To inform the controller without delay of the breach
- To inform, in the context of a general or specific leave, of the recruitment of another processor

6. What measures can the processor take in order to satisfy the requirement of confidentiality in relation to the staff it employs?

The processor must recruit staff with integrity and knowledge and ensure that only properly authorised and trained in personal data protection personnel process personal data while carrying out their work in the processor's company. The staff referred to above shall make a written declaration of confidentiality.

For example, the following may be envisaged:

a) use of a mechanism/system to control access based on roles assigned to staff (role-based access control mechanism);

b) granting and modifying the corresponding classified access rights on the basis of the minimum privileged principle, the 'need-to-know' principle and the delegation of the relevant tasks and responsibilities;

c) establishment of specific rules for users with privileged access and increased rights;

d) a procedure for the revocation of rights in the event of a user leaving or changing tasks and responsibilities.

7. Under what conditions can sub-processors be used by the processor (under what conditions can the processor hire another processor ('subcontractor') for the processing?

The processor shall recruit another processor ('subcontractor') only with prior, specific and written permission of the controller.

Alternatively, the processor may recruit another processor ('subcontractor') on the basis of a general authorisation from the controller having the right to object. In that case, it shall inform the controller in a timely manner (and in detail) of any intended changes relating to the addition or replacement of the other processors. The controller shall have the right, within a specified period of time, to object, in whole or in part, to the recruitment or replacement of subcontractors.

The processor shall ensure and guarantee that the subcontractor is subject through a contract concluded with it to the same obligations laid down in law and in the contract between a controller and processor and that it is able to meet the requirements of the processing of personal data. At the request of the controller, the processor must inform the controller of the terms of the contract which it intends to conclude with the third party-subcontractor. This contract may not invalidate the conditions for the processing of personal data resulting from the contract between the controller and the processor.

Where the subcontractor fails to fulfil its data protection obligations, the processor shall remain fully accountable to the controller for the fulfilment of the subcontractor's obligations.

[Place of processing/transfer of data to third parties — third countries and under what conditions]

8. Is the use of cloud computing/provider of internet services/social media whose servers are located in a third country e.g. USA, India, etc. by processors legitimate — acceptable?

In principle, no. Any transfer of personal data to third countries or international organisations by the processor shall only take place on the basis of recorded instructions from the controller. Also, the conditions set out in the GDPR, i.e. an EU adequacy decision, have to be met, or standard data protection clauses (standard contractual

clauses) or binding corporate rules must have been concluded. The EU has so far adopted an adequacy decision for the following countries only: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. There is no adequacy decision for the US.

9. What is the role of the processor in relation to the notification of a data breach?

In the event of a personal data breach, which is first brought to the attention of the processor, the processor shall inform the controller without delay from the moment it becomes aware of that breach in order to enable the controller to comply with the obligations to notify the personal data breach and any information to the affected persons in accordance with the GDPR. If it receives a request from the controller for a personal data breach incident, it shall assist in providing the required data and information, communicating the incident to the competent supervisory authority and taking all reasonable measures to limit the impact and prevent a recurrence of the breach.

Information to detect and manage breaches is available here.

Employee awareness leaflet for breach incidents is available here.

10. When does the processor delete and/or return the data to the controller?

Upon termination of the provision of personal data processing services, the processor shall erase or return the personal data, as provided for in the contract between controller-processor. Where it is only provided for the data to be returned to the controller, the processor shall delete any copies kept during the period of validity of the contract.

A template for the destruction of a file with personal data is available here and a file destruction protocol template is available here.

11. I have employed a security — video surveillance and/or medical service company for the company's staff. Should the contract with this company-processor include a term relating to the designation of a Data Protection Officer (DPO)?

Yes, a relevant term must be included in the contract between controller-processor providing that the processor discloses the name and contact details of the Data Protection Officer (DPO) to the controller in case it is legally obliged (Art. 37 GDPR) to appoint a Data Protection Officer (DPO).

12. How is the processor's compliance with the GDPR and the controller's instructions demonstrated?

The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR and in the contractual text between them and shall allow and facilitate controls, including inspections, carried out by the controller or by another auditor mandated by the controller.

5.9.2 General template Appendix regarding data processing to a signed contract between SME and processor

Annex

Personal Data Processing

Between Controller and Processor as a Company providing services on ……..

In Athens today, between the parties:

the company by the name……[98](and distinctive title……[99]) established in..... (street..... no. ..... tel..... e-mail.....) and legally represented by..... (hereinafter referred to as "the Controller") and

the company by the name..... established in..... and legally represented by..... (hereinafter referred to as "Processor"),

Whereas:

(a) The parties have signed the contract on ..... [date] (hereinafter referred to as "the main contract"), to which this forms an annex;

(b) With effect from 25 May 2018, 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 "Regulation" or "GDPR") was implemented and also Law 4624/2019 lays down implementing measures for the Regulation;

(c) The Controller processes personal data in the course of its business activity and decides on the purposes, methods and means of the processing of personal data;

(d) The Processor processes personal data on behalf of and in accordance with the instructions of the Controller;

recognise, agree and mutually accept the following:

1. Preamble

1.1. This Annex sets out the rights and obligations of the Controller and the Processor when processing personal data on behalf of the controller (hereinafter "Personal Data"). The Contracting Parties agree to the terms of this Annex in order to meet the requirements of the Regulation and to ensure the protection of the rights of data subjects.

1.2. The terms of this Agreement shall take precedence over any similar provisions contained in other agreements between the Parties.

2. Rights and obligations of the Controller

2.1 The Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the Regulation (see Article 24 GDPR), the applicable national and European data protection provisions and this Annex.

2.2 The Controller has the right and obligation to make decisions on the purposes and means of the processing of Personal Data.

[98]Complete full legal name or name in case of sole proprietorship.

[99] Fill in the distinctive title (trade name) of the company, if any.

2.3 The Controller is responsible, inter alia, for ensuring that the processing of Personal Data assigned to the Processor has a legal basis.

3. Obligations of the Processor

3.1 The Processor shall process Personal Data on behalf of the Controller only on the basis of the instructions of the Controller listed in this Annex, unless it is required to do so under national or European law. The Controller may also provide subsequent instructions throughout the processing of the Personal Data, but such instructions will always be recorded and kept in writing (or in electronic form) in conjunction with this Annex.

3.2 The Processor shall use the Personal Data in accordance with and only for the purpose set out in this Annex and only in the manner and to the extent necessary for the provision of its services to the Controller, and shall inform the Controller without delay if, in its opinion, the instructions provided by the latter are contrary to the GDPR or to the applicable national or European data protection provisions.

The processor shall communicate the name and contact details of the Data Protection Officer (DPO) to the controller if it is legally obliged (Article 37 GDPR) to appoint a Data Protection Officer (DPO).

3.3 Information about the processing

3.3.1 The purpose of the processing of personal data by the Processor on behalf of the Controller is..... [specify the type of service provided] indicatively providing accounting services

3.3.2 Processing of Personal Data by the Processor on behalf of the Controller relates mainly to..... [describe the type of activity] indicatively: employee payroll management, tax data-invoicing management

3.3.3 The processing shall include the following types of personal data relating to data subjects: [indicate type of data] Identification, contact details, ...

3.3.4 The processing shall include the following categories of data subjects:

Indicatively employees, customers, suppliers.....

3.3.5 Processing of Personal Data by the Processor on behalf of the Controller may be carried out from the implementation of this Annex for the same period of validity.

3.4. The Processor will keep a record of the activities of all individual categories of processing carried out on behalf of the Controller in accordance with the provisions of the legislation on the protection of personal data. This file will be made available to the Controller.

4. Confidentiality

4.1 The Processor shall grant access to Personal Data processed on behalf of the Controller exclusively to persons under its supervision who have undertaken to maintain confidentiality or are under the appropriate regulatory obligation of confidentiality and only when there is a “need to know” of the Personal Data in order to be able to provide its services to the Controller in accordance with the main contract. The list of persons to whom a right of access has been granted shall be subject to periodic review. On the basis of this review, access

to Personal Data may be revoked if it is no longer necessary, and therefore such persons will no longer be able to access the Personal Data.

4.2 At the request of the Controller, the Processor shall prove that such persons under its supervision are subject to the aforementioned obligation of confidentiality.

4.3 The Processor shall take all reasonable measures to ensure adequate training of its personnel processing Personal Data with regard to compliance with this Annex and applicable legislation on the protection of personal data.

5. Security of processing

5.1 Article 32 GDPR states that, taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure an appropriate level of security against risks. The Controller shall assess the risks posed by the processing to the rights and freedoms of natural persons and shall take measures to mitigate those risks. Depending on the significance of the risks, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis;

c. the ability to restore the availability and access to personal data in due time in the event of a physical or technical incident;

d. procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

5.2 With regard to the level of security of the processing to be carried out by the Processor, account should be taken of the fact that the processing involves a large amount of Personal Data, some of which may fall under Article 9 GDPR for 'special categories of personal data', which is why a 'high' level of security should be established.

5.3 In any case, the Processor shall apply as a minimum the following measures agreed with the Controller:

List of key personal data security measures

[the above link to the list is available, which you can enrich with additional measures and attach to this Annex. These additional measures may concern the following categories:]

[DESCRIBE THE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE THE REQUIREMENTS FOR ENSURING THE CONFIDENTIALITY, CONTINUITY, AVAILABILITY AND RELIABILITY OF SYSTEMS AND PROCESSING SERVICES ON A CONTINUOUS BASIS]

[DESCRIBE THE REQUIREMENTS FOR RECOVERABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A NATURAL OR TECHNICAL EVENT]

[DESCRIBE THE REQUIREMENTS FOR THE PROCEDURE FOR REGULAR TESTING, ASSESSMENT AND EVALUATION OF THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SAFETY OF PROCESSING]

[DESCRIBE THE REQUIREMENTS FOR INTERNET ACCESS]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS DURING TRANSFER]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS AT STORAGE]

[DESCRIBE THE MATERIAL SECURITY REQUIREMENTS OF THE PLACES WHERE PERSONAL DATA ARE PROCESSED]

[DESCRIBE THE REQUIREMENTS FOR WORK AT HOME/DISTANCE]

[DESCRIBE THE CONNECTION REQUIREMENTS]

5.4 In accordance with Article 32 of the GDPR, the Processor shall also assess — independently of the Controller — the risks posed by the processing to the rights and freedoms of natural persons and take measures to mitigate those risks. To this end, the Controller shall provide the Processor with all information necessary to identify and evaluate these risks.

5.5 In addition, the Processor assists the Controller in ensuring compliance with the Controller's obligations under Article 32 GDPR, including by providing the Controller with information on the technical and organisational measures already implemented by the Processor in accordance with Article 32 GDPR, as well as any other information necessary for the Controller to comply with its obligation under Article 32 GDPR. If subsequently — in the assessment of the Controller — mitigation of the identified risks requires further measures to be taken by the Processor, in addition to those already applied in accordance with Article 32 GDPR, the Controller shall specify those additional measures to be applied by an amendment to this Article.

6. Use of processing subcontractors

6.1 The Processor should meet the requirements set out in Article 28(2) and (4) GDPR in order to recruit another processor (sub-processor).

6.2 The Processor therefore does not employ another processor (sub-processor) to fulfil its obligations under the main contract without the prior specific written permission of the Controller.

6.3 The Processor shall submit the request for a specific permit at least one month before the sub-processor is recruited. The list of sub-processors already authorised by the Controller is set out in the following paragraph.

[specify time period, indicatively one month]

6.4 Authorised sub-processors

Upon the entry into force of this Annex, the Controller shall authorise the use of the following sub-processors for the processing described in respect of that contractor:

NAME	ADDRESS	DESCRIPTION OF THE PROCESSING

The Processor shall not be entitled to hire a sub-processor for processing other than that agreed, or to have the processing described as carried out by another sub-processor, except under conditions 6.2 and 6.3 hereof.

6.5 Where the Processor employs a sub-processor to carry out specific processing activities on behalf of the Controller, the same data protection obligations set out in this Annex shall be imposed on the sub-processor by means of a contract or other legal act in accordance with national or European law, in particular in order to provide sufficient assurances on the application of appropriate technical and organisational measures to ensure that the processing meets the requirements of this Annex and the GDPR. Consequently, the Processor must (a) before hiring any new sub-processor, carry out a due diligence process to ensure that the sub-processor is capable of ensuring the level of protection of Personal Data provided for in this Annex and the GDPR and (b) ensure that its sub-processors are contractually bound by the same obligations relating to the processing of the Personal Data as those binding the Processor in accordance with this Annex and the GDPR.

6.6 A copy of the sub-processing agreement and subsequent amendments shall be submitted to the Controller upon request to enable the Controller to ensure that the sub-processor is subject to the same data protection obligations as set out in this Annex. Clauses on business matters that do not affect the legal content of the sub-processing agreement with regard to data protection shall not be submitted to the Controller.

6.7 If the sub-processor fails to fulfil its obligations relating to the protection of personal data, the Processor shall remain fully accountable to the Controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR, in particular those provided for in Articles 79 and 82 GDPR, vis-à-vis the Controller and the Processor, including the sub-processor.

7. Place of processing — Transfer of data to third countries

7.1 The processing of personal data under this Annex may not be carried out in locations other than the EU and EEA without the prior written authorisation of the Controller.

7.2 Any transfer of Personal Data to third countries, for which the EU has issued an adequacy decision and where the standard contractual clauses are applied, or to international organizations, by the Processor shall only take place on the basis of recorded instructions from the Controller and always in compliance with Chapter V of the GDPR.

7.3 Therefore, without recorded instructions from the Controller, the Processor cannot, under this Annex:

a. transfer personal data to a controller or processor in a third country or an international organisation;

b. entrust the processing of personal data to a sub-processor in a third country;

c. process personal data itself in a third country.

8. Assistance to the controller

8.1 Taking into account the nature of the processing, the Processor provides assistance to the Controller with appropriate technical and organisational measures, to the extent possible, to fulfil the obligations of the Controller to respond to requests for the exercise of the data subject's rights provided for in the GDPR and in Law 4624/2019. This implies that the Processor provides assistance, to the extent possible, to the Controller to fulfil the rights of data subjects as provided for in Articles 12-22 GDPR.

8.2 In addition to the obligation of the Processor to assist the Controller pursuant to Article 5.4 hereof, the Processor shall also assist the Controller, taking into account the nature of the processing and the information available to the Processor to ensure compliance with:

a. the controller's obligation to notify without delay and, if possible, within 72 hours of becoming aware of the personal data breach, the personal data breach, unless the personal data breach is unlikely to cause a risk to the rights and freedoms of natural persons;

b. the controller's obligation to communicate without delay the personal data breach to the data subject where the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons;

c. the obligation of the controller to carry out, where appropriate, an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment);

d. the obligation of the controller to consult the competent supervisory authority prior to processing where the data protection impact assessment indicates that the processing would cause a high risk in the absence of risk mitigation measures by the Controller.

8.3 To the extent possible — within the scope and extent of the assistance specified below — the Processor shall assist the Controller in accordance with paragraphs 8.1. and 8.2 above by taking the following technical and organisational measures:

[DESCRIBE THE SCOPE AND EXTENT OF ASSISTANCE TO BE PROVIDED BY THE PROCESSOR]

[DESCRIBE THE SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES TO BE TAKEN BY THE PROCESSOR IN ORDER TO ASSIST THE CONTROLLER]

9. Data breach notification

9.1 In the event of a personal data breach, the Processor shall inform the Controller of the personal data breach without delay from the moment it becomes aware of the breach.

9.2 The Controller's notification by the Processor shall take place without delay and, in any event, within 24 hours after the Processor becomes aware of the personal data breach, in order to enable the Controller to comply with the obligations to notify the personal data breach pursuant to Articles 33 and, where applicable, 34 GDPR.

[More time can be specified than 24 hours but less than 72 hours.]

9.3 In accordance with Article 8(2)(a), the Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority. This means that the Processor is obliged to assist in obtaining the information as provided for in Article 33(3) GDPR.

9.4 If the Processor is unable to provide all the information referred to in paragraph 9.3 within the timeframes provided for, then before the expiry of the above mentioned timeframe, it shall explain to the Controller the reasons for the delay, providing an indication of when it is expected to be able to provide the relevant details (possibly also occasionally), and inform the Controller at regular intervals of these matters.

9.5 Following the detection of the data breach, the Processor will (a) conduct an investigation into the data breach without undue delay and provide information to the Controller about the breach, (b) take reasonable measures to limit the impact and minimise the damage caused by the data breach, including assisting the Controller in remedying or limiting the potential damage from the breach, to the extent that such remedy or restriction is under the control of the Processor, as well as reasonable measures to prevent a recurrence of the data breach and (c) cooperate fully with the Controller to develop and implement an action plan to address the breach.

10. Erasure and return of data

10.1 Personal data shall be stored for the entire period of validity of the main contract between the parties and subsequently automatically erased by the processor, unless a specific legislative or regulatory provision requiring the data to be stored for a shorter period applies.

10.2 Upon termination of the provision of personal data processing services, the Processor is obliged, at the choice of the Controller and in accordance with its instructions, either (a) to return all Personal Data to the Controller, or (b) to delete all Personal Data, providing in any case within a specified period of time [indicatively mentioned] of fifteen days after the end of the cooperation; written certification to the Controller that the processor and any of its sub-processors no longer keep copies of personal data obtained by virtue of the main contract, unless a provision of national or European law requires further storage of the Personal Data.

10.3 In the event that, despite the expiration of this Annex, the applicable law requires the storage of any Personal Data by the Processor, the Processor shall (a) inform the Controller of this requirement, in which case it will become the Controller for such limited purposes, and (b) ensure that the Data is processed only to the extent necessary to comply with the applicable law requiring storage, to the exclusion of any other purpose.

11. Control and inspection

11.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and this Annex and shall permit and facilitate audits, including inspections, carried out by the Controller or by another auditor authorised by the Controller.

The Controller or the representative of the Controller [specify the period of time, indicatively every five months] shall carry out an inspection of the sites where the Processor carries out the processing of the Personal Data, including the physical facilities as well as the systems used and related to the processing in order to verify the Compliance with the GDPR, the applicable data protection provisions and this Annex.

In addition to the scheduled inspection, the Controller may inspect the Processor when it considers that such an inspection is necessary.

11.2 The Processor shall be obliged to grant the supervisory authorities, which under the applicable law have access to the premises of the Controller and the Processor, or to representatives acting on behalf of those

supervisory authorities, access to the physical premises of the processor on presentation of appropriate identification documents.

12. Entry into force and expiry

12.1 This Annex shall enter into force on the date of its signature by both Parties.

12.3 This Annex shall apply throughout the provision of the services of the main contract by the Processor to the Controller.

12.4 If the provision of personal data processing services expires and the Personal Data is deleted or returned to the Controller in accordance with Article 10 of these presents, either Party may terminate this document by written notice.

5.9.3 Specific template Appendix for processors that provide services of promoting products and services

Annex

Personal Data Processing

between Controller and Processor as a Company

providing product and service promotion services

In Athens today, between the parties:

The company by the name……[100] (and distinctive title……[101]) established in ..... (street....., no. …… tel..... e-mail: .....) and legally represented by ..... (hereinafter referred to as "the Controller") and

the company by the name ..... established in..... and legally represented by..... (hereinafter referred to as "the Processor"),

Whereas:

(a) The parties have signed the contract on ..... [date] (hereinafter referred to as "the main contract"), to which this forms an annex.

(b) With effect from 25 May 2018, 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 "Regulation" or "GDPR") was implemented and also Law 4624/2019 lays down implementing measures for the Regulation.

(c) The Controller processes personal data in the course of its business activity and decides on the purposes, methods and means of the processing of personal data;

[100] Complete full legal name or name in case of sole proprietorship.
[101] Fill in the distinctive title (trade name) of the company, if any.

(d) The Processor processes personal data on behalf of and in accordance with the instructions of the Controller;

recognise, agree and mutually accept the following:

2. Preamble

2.1. This Annex sets out the rights and obligations of the Controller and the Processor when processing personal data on behalf of the controller (hereinafter "Personal Data"). The Contracting Parties agree to the terms of this Annex in order to meet the requirements of the Regulation and to ensure the protection of the rights of data subjects.

2.2. The terms of this Agreement shall take precedence over any similar provisions contained in other agreements between the Parties.

2. Rights and obligations of the Controller

2.1 The Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the Regulation (see Article 24 GDPR), the applicable national and European data protection provisions and this Annex.

2.2 The Controller has the right and obligation to make decisions on the purposes and means of the processing of Personal Data.

2.3 The Controller is responsible, inter alia, for ensuring that the processing of Personal Data assigned to the Processor has a legal basis.

3. Obligations of the Processor

3.1 The Processor shall process Personal Data on behalf of the Controller only on the basis of the instructions of the Controller listed in this Annex, unless it is required to do so under national or European law. The Controller may also provide subsequent instructions throughout the processing of the Personal Data, but such instructions will always be recorded and kept in writing (or in electronic form) in conjunction with this Annex.

3.2 The Processor shall use the Personal Data in accordance with and only for the purpose set out in this Annex and only in the manner and to the extent necessary for the provision of its services to the Controller, and shall inform the Controller without delay if, in its opinion, the instructions provided by the latter are contrary to the GDPR or to the applicable national or European data protection provisions.

The Processor (DPO) shall communicate the name and contact details of the Data Protection Officer (DPO) to the controller if it is legally obliged (Article 37 GDPR) to appoint a Data Protection Officer (DPO).

3.3 Information about the processing

3.3.1 The purpose of personal data processing by the Processor on behalf of the Controller is to communicate with customers or potential customers of the Controller for the purpose of the promotion of products and/or services.

3.3.2 Processing of Personal Data by the Processor on behalf of the Controller mainly concerns informing the customers of the Controller or reaching potential customers on behalf of the Controller by electronic means and

recording the result of the communication for further evaluation and processing by the Controller and the Processor.

3.3.3 The processing includes the following types of personal data relating to the Controller's customers: Identification details, contact details, data generated by the communications, such as date and duration of call, date and time of sending of the message [to be amended accordingly].

In the case of telephone calls involving human intervention to potential customers of the Controller, the processing shall include telephone connection numbers first and once the communication has been achieved and the recipient is interested the caller informs the recipient of its identification details [to be amended accordingly].

In the case of communications by electronic means (email, SMS, fax, voice mail, Viber, WhatsApp, etc.), with the exception of calls from persons but including calls without human intervention, to potential customers, the processing includes name and contact details, with the prior consent of the potential customer [to be amended accordingly].

The processing of potential customers' data includes the data generated by the relevant communications such as the date and duration of the call, the date and time of sending the message [to be amended accordingly].

The Processor should process the data resulting from the communications made on behalf of the Controller, such as the date and time of the call, in accordance with the obligations arising from the specific legal and regulatory framework.

3.3.4 The processing shall include the following categories of data subjects:

- customers of the Controller
- potential customers of the Controller

3.3.5 Processing of Personal Data by the Processor on behalf of the Controller may be carried out from the implementation of this Annex for the same period of validity.

3.4. The Processor will keep a record of all individual categories of processing carried out on behalf of the Controller in accordance with the legislation on the protection of personal data. This file will be made available to the Controller.

3.5. Before carrying out communication activities for the marketing of products and/or services, as well as for any kind of advertising purposes, the Processor must apply the specific legal and regulatory framework and consult the statutory registers, such as the Register of article 11 of Law 3471/2006, as well as the lists including any objections submitted by customers and/or potential customers of the Controller and/or the consents of its customers.

3.6 Before carrying out communication activities for the marketing of products and/or services, as well as for any kind of advertising purposes to potential customers by electronic means (email, SMS, MMS, instant messaging services, electronic messaging services such as social networking pages, calls without human intervention), the Processor has the prior written consent of the recipient. Consent may be given electronically (see Authority Directive 2/2011) and must be given in full knowledge, after appropriate information, and recorded in a secure manner by the Controller.

4. Confidentiality

4.1 The Processor shall grant access to Personal Data processed on behalf of the Controller exclusively to persons under its supervision who have undertaken to maintain confidentiality or are under the appropriate regulatory obligation of confidentiality and only when there is a “need to know” of the Personal Data in order to be able to provide its services to the Controller in accordance with the main contract. The list of persons to whom a right of access has been granted shall be subject to periodic review. On the basis of this review, access to Personal Data may be revoked if it is no longer necessary, and therefore such persons will no longer be able to access the Personal Data.

4.2 At the request of the Controller, the Processor shall prove that such persons under its supervision are subject to the aforementioned obligation of confidentiality.

4.3 The Processor shall take all reasonable measures to ensure adequate training of its personnel processing Personal Data with regard to compliance with this Annex and applicable legislation on the protection of personal data.

5. Security of processing

5.1 Article 32 GDPR states that, taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure an appropriate level of security against risks. The Controller shall assess the risks posed by the processing to the rights and freedoms of natural persons and shall take measures to mitigate those risks. Depending on the significance of the risks, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis;

c. the ability to restore the availability and access to personal data in due time in the event of a physical or technical incident;

d. procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

5.2 With regard to the level of security of the processing to be carried out by the Processor, account should be taken of the fact that the processing involves a large amount of Personal Data, some of which may fall under Article 9 GDPR for ‘special categories of personal data’, which is why a ‘high’ level of security should be established.

5.3 The Processor is henceforth entitled and obliged to take decisions on the technical and organisational security measures to be implemented in order to achieve the necessary (and agreed) level of data security. In any case, however, the Processor shall at least apply the following measures agreed with the Controller:

List of key personal data security measures

[the above link to the list is available, which you can enrich with additional measures and attach to this Annex. These additional measures may concern the following categories:]

[DESCRIBE THE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE THE REQUIREMENTS FOR ENSURING THE CONFIDENTIALITY, CONTINUITY, AVAILABILITY AND RELIABILITY OF SYSTEMS AND PROCESSING SERVICES ON A CONTINUOUS BASIS]

[DESCRIBE THE REQUIREMENTS FOR RECOVERABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A NATURAL OR TECHNICAL EVENT]

[DESCRIBE THE REQUIREMENTS FOR THE PROCEDURE FOR REGULAR TESTING, ASSESSMENT AND EVALUATION OF THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SAFETY OF PROCESSING]

[DESCRIBE THE REQUIREMENTS FOR INTERNET ACCESS]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS DURING TRANSFER]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS AT STORAGE]

[DESCRIBE THE MATERIAL SECURITY REQUIREMENTS OF THE PLACES WHERE PERSONAL DATA ARE PROCESSED]

[DESCRIBE THE REQUIREMENTS FOR WORK AT HOME/DISTANCE]

[DESCRIBE THE CONNECTION REQUIREMENTS]

5.4 In accordance with Article 32 of the GDPR, the Processor shall also assess — independently of the Controller — the risks posed by the processing to the rights and freedoms of natural persons and take measures to mitigate those risks. To this end, the Controller shall provide the Processor with all information necessary to identify and evaluate these risks.

5.5 In addition, the Processor assists the Controller in ensuring compliance with the Controller's obligations under Article 32 GDPR, including by providing the Controller with information on the technical and organisational measures already implemented by the Processor in accordance with Article 32 GDPR, as well as any other information necessary for the Controller to comply with its obligation under Article 32 GDPR. If subsequently — in the assessment of the Controller — mitigation of the identified risks requires further measures to be taken by the Processor, in addition to those already applied in accordance with Article 32 GDPR, the Controller shall specify those additional measures to be applied by an amendment to this Article.

6. Use of processing subcontractors

6.1 The Processor should meet the requirements set out in Article 28(2) and (4) GDPR in order to recruit another processor (sub-processor).

6.2 The Processor therefore does not employ another processor (sub-processor) to fulfil its obligations under the main contract without the prior specific written permission of the Controller.

6.3 The Processor shall recruit sub-processors only with the specific prior authorisation of the Controller. The Processor shall submit the request for a specific permit at least one month before the sub-processor is recruited. The list of sub-processors already authorised by the Controller is set out in the following paragraph.

[specify time period, indicatively one month]

6.4 Authorised subprocessors

Upon the entry into force of this Annex, the Controller shall authorise the use of the following sub-processors for the processing described in respect of that contractor:

NAME	ADDRESS	DESCRIPTION OF THE PROCESSING

The Processor shall not be entitled, without the express written permission of the Controller, to hire a sub-processor for processing other than that agreed or to entrust another sub-processor with the execution of the processing described.

6.5 Where the Processor employs a sub-processor to carry out specific processing activities on behalf of the Controller, the same data protection obligations set out in this Annex shall be imposed on the sub-processor by means of a contract or other legal act in accordance with national or European law, in particular in order to provide sufficient assurances on the application of appropriate technical and organisational measures to ensure that the processing meets the requirements of this Annex and the GDPR. Consequently, the Processor must (a) before hiring any new sub-processor, carry out a due diligence process to ensure that the sub-processor is capable of ensuring the level of protection of Personal Data provided for in this Annex and the GDPR and (b) ensure that its sub-processors are contractually bound by the same obligations relating to the processing of the Personal Data as those binding the Processor in accordance with this Annex and the GDPR.

6.6 A copy of the sub-processing agreement and subsequent amendments shall be submitted to the Controller upon request to enable the Controller to ensure that the sub-processor is subject to the same data protection obligations as set out in this Annex. Clauses on business matters that do not affect the legal content of the sub-processing agreement with regard to data protection shall not be submitted to the Controller.

6.7 If the sub-processor fails to fulfil its obligations relating to the protection of personal data, the Processor shall remain fully accountable to the Controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR, in particular those provided for in Articles 79 and 82 GDPR, vis-à-vis the Controller and the Processor, including the sub-processor.

7. Place of processing — Transfer of data to third countries

7.1 The processing of personal data under this Annex may not be carried out in locations other than the EU and the EEA area without the prior written permission of the Controller.

7.2 Any transfer of Personal Data by the Processor to third countries, for which the EU has issued an adequacy decision and where the standard contractual clauses are applied, or to international organizations, shall only take place on the basis of recorded instructions from the Controller and always in compliance with Chapter V of the GDPR.

7.3 Therefore, without recorded instructions from the Controller, the Processor cannot, under this Annex:

a. transfer personal data to a controller or processor in a third country or an international organisation;

b. entrust the processing of personal data to a sub-processor in a third country;

c. process personal data itself in a third country.

8. Assistance to the controller

8.1 Taking into account the nature of the processing, the Processor provides assistance to the Controller with appropriate technical and organisational measures, to the extent possible, to fulfil the obligations of the Controller to respond to requests for the exercise of the data subject's rights provided for in the GDPR and in Law 4624/2019. This implies that the Processor assists the Controller, to the extent possible, to satisfy:

a. the right to information of the data subject when the personal data are collected from the data subject

b. the right to information of the data subject where the personal data have not been collected by the data subject

c. the data subject's right of access

d. the right to rectification

e. the right to erasure ('right to be forgotten')

f. the right to restrict processing

g. the obligation to notify concerning rectification or erasure of personal data or restriction of processing

h. the right to data portability

i. the right to object

j. the right of the data subject not to be subject to a decision taken solely on the basis of automated processing, including profiling.

8.2 In addition to the obligation of the Processor to assist the Controller pursuant to Article 5.4 hereof, the Processor shall also assist the Controller, taking into account the nature of the processing and the information available to the Processor to ensure compliance with:

a. the controller's obligation to notify without delay and, if possible, within 72 hours of becoming aware of the personal data breach, the personal data breach, unless the personal data breach is unlikely to cause a risk to the rights and freedoms of natural persons;

b. the controller's obligation to communicate without delay the personal data breach to the data subject where the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons;

c. the obligation of the Controller to carry out, where appropriate, an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment);

d. the obligation of the Controller to consult the competent supervisory authority prior to processing where the data protection impact assessment indicates that the processing would cause a high risk in the absence of risk mitigation measures by the Controller.

8.3 To the extent possible — within the scope and extent of the assistance specified below — the Processor shall assist the Controller in accordance with paragraphs 8.1. and 8.2 above by taking the following technical and organisational measures:

[DESCRIBE THE SCOPE AND EXTENT OF ASSISTANCE TO BE PROVIDED BY THE PROCESSOR]

[DESCRIBE THE SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES TO BE TAKEN BY THE PROCESSOR IN ORDER TO ASSIST THE CONTROLLER]

9. Data breach notification

9.1 In the event of a personal data breach, the Processor shall inform the Controller of the personal data breach without delay from the moment it becomes aware of the breach.

9.2 The Controller's notification by the Processor shall take place without delay and, in any event, within 24 hours after the Processor becomes aware of the personal data breach, in order to enable the Controller to comply with the obligations to notify the personal data breach pursuant to Articles 33 and, where applicable, 34 GDPR.

[More time can be specified than 24 hours but less than 72 hours.]

9.3 In accordance with Article 8(2)(a), the Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority. This means that the Processor is obliged to assist in securing the information listed below, which, pursuant to Article 33(3) GDPR, is reported in the controller's notification to the competent supervisory authority:

a. the nature of the personal data, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records affected;

b. possible consequences of the personal data breach;

c. measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

9.4 If the Processor is unable to provide all the information referred to in paragraph 9.3 within the timeframes provided for, then before the expiry of the above mentioned timeframe, it shall explain to the Controller the reasons for the delay, providing an indication of when it is expected to be able to provide the relevant details (possibly also occasionally), and inform the Controller at regular intervals of these matters.

9.5 Following the detection of the data breach, the Processor will (a) conduct an investigation into the data breach without undue delay and provide information to the Controller about the breach, (b) take reasonable measures to limit the impact and minimise the damage caused by the data breach, including assisting the Controller in remedying or limiting the potential damage from the breach, to the extent that such remedy or restriction is under the control of the Processor, as well as reasonable measures to prevent a recurrence of the

data breach and (c) cooperate fully with the Controller to develop and implement an action plan to address the breach.

10. Erasure and return of data

10.1 The Personal Data of the Controller's customers or potential customers shall be retained by the Processor during the duration of the main contract for the period provided for by the specific legal and regulatory framework.

10.2 Upon termination of the provision of personal data processing services, the Processor shall return all personal data to the Controller and delete existing copies, providing within a specified period of fifteen days after the end of the cooperation, a written certification to the Controller that the processor and each of his sub-processors has fully complied with this paragraph, unless a provision of national or European law requires further storage of the Personal Data.

10.3 In the event that, despite the expiration of this Annex, the applicable law requires the storage of any Personal Data by the Processor, the Processor shall (a) inform the Controller of this requirement, in which case it will become the Controller for such limited purposes, and (b) ensure that the Data is processed only to the extent necessary to comply with the applicable law requiring storage, to the exclusion of any other purpose.

11. Control and inspection

11.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and this Annex and shall permit and facilitate audits, including inspections, carried out by the Controller or by another auditor authorised by the Controller.

The Controller or the representative of the Controller [specify the period of time, indicatively every five months] shall carry out an inspection of the sites where the Processor carries out the processing of the Personal Data, including the physical facilities as well as the systems used and related to the processing in order to verify the Compliance with the GDPR, the applicable data protection provisions and this Annex.

In addition to the scheduled inspection, the Controller may inspect the Processor when it considers that such an inspection is necessary.

11.2 The Processor shall be obliged to grant the supervisory authorities, which under the applicable law have access to the premises of the Controller and the Processor, or to representatives acting on behalf of those supervisory authorities, access to the physical premises of the processor on presentation of appropriate identification documents.

12. Entry into force and expiry

12.1 This Annex shall enter into force on the date of its signature by both Parties.

12.3 This Annex shall apply throughout the provision of the services of the main contract by the Processor to the Controller.

12.4 If the provision of personal data processing services expires and the Personal Data is deleted or returned to the Controller in accordance with Article 10 of these presents, either Party may terminate this document by written notice.

5.9.4 Specific template Appendix for processors that are cloud service providers

Annex

Personal Data Processing

Between Controller and Processor as cloud service provider

In Athens today, between the parties:

the company by the name[102] (and distinctive title[103] ……) ..... established in..... (street..... no. ..... tel ..... e-mail.....) and legally represented by..... (hereinafter referred to as "the Controller") and

the company by the name ..... established in..... and legally represented by..... (hereinafter referred to as "Processor"),

Whereas:

(a) The parties have signed the contract on ..... [date] (hereinafter referred to as "the main contract"), to which this forms an annex.

(b) With effect from 25 May 2018, 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 "Regulation" or "GDPR") was implemented and also Law 4624/2019 lays down implementing measures for the Regulation.

(c) The Controller processes personal data in the course of its business activity and decides on the purposes, methods and means of the processing of personal data;

(d) The Processor processes personal data on behalf of and in accordance with the instructions of the Controller;

recognise, agree and mutually accept the following:

3. Preamble

3.1. This Annex sets out the rights and obligations of the Controller and the Processor when processing personal data on behalf of the controller (hereinafter "Personal Data"). The Contracting Parties agree to the terms of this Annex in order to meet the requirements of the Regulation and to ensure the protection of the rights of data subjects.

3.2. The terms of this Agreement shall take precedence over any similar provisions contained in other agreements between the Parties.

2. Rights and obligations of the Controller

[102] Complete full legal name or name in case of sole proprietorship.

[103] Fill in the distinctive title (trade name) of the company, if any.

2.1 The Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the Regulation (see Article 24 GDPR), the applicable national and European data protection provisions and this Annex.

2.2 The Controller has the right and obligation to make decisions on the purposes and means of the processing of Personal Data.

2.3 The Controller is responsible, inter alia, for ensuring that the processing of Personal Data assigned to the Processor has a legal basis.

3. Obligations of the Processor

3.1 The Processor shall process Personal Data on behalf of the Controller only on the basis of the instructions of the Controller listed in this Annex, unless it is required to do so under national or European law. The Controller may also provide subsequent instructions throughout the processing of the Personal Data, but such instructions will always be recorded and kept in writing (or in electronic form) in conjunction with this Annex.

3.2 The Processor shall use the Personal Data in accordance with and only for the purpose set out in this Annex and only in the manner and to the extent necessary for the provision of its services to the Controller, and shall inform the Controller without delay if, in its opinion, the instructions provided by the latter are contrary to the GDPR or to the applicable national or European data protection provisions.

The processor shall communicate the name and contact details of the Data Protection Officer (DPO) to the controller if it is legally obliged (Article 37 GDPR) to appoint a Data Protection Officer (DPO).

3.3 Information about the processing

3.3.1 The purpose of the processing of Personal Data by the Processor on behalf of the Controller is to host applications of the information system, portal, database(s) of the Controller on the Cloud of the Processor. [mentioned indicatively — modify accordingly]

3.3.2 Processing of Personal Data by the Processor on behalf of the Controller mainly concerns the storage of the applications and data of the Controller as well as the keeping of backups of the data [mentioned indicatively — modify accordingly]

3.3.3 The processing shall include the following types of personal data relating to data subjects: Identification details, contact details, web browsing information on the Controller's portal, user account details in the information system, user history in the information system, any documents entered in the system or databases (this may include special categories of data within the meaning of Article 9 GDPR) [mentioned indicatively — modify accordingly]

3.3.4 The processing shall include the following categories of data subjects: Employees, customers and suppliers of the Controller, visitors to the Controller's portal, users of the Controller's IT system [mentioned indicatively — modify accordingly].

3.3.5 Processing of Personal Data by the Processor on behalf of the Controller may be carried out as from the implementation of this Annex for the same period of validity.

3.4. The Processor will keep a record of the activities of all individual categories of processing carried out on behalf of the Controller in accordance with the provisions of the legislation on the protection of personal data. This file will be made available to the Controller.

4. Confidentiality

4.1 The Processor shall grant access to Personal Data processed on behalf of the Controller exclusively to persons under its supervision who have undertaken to maintain confidentiality or are under the appropriate regulatory obligation of confidentiality and only when there is a "need to know" of the Personal Data in order to be able to provide its services to the Controller in accordance with the main contract. The list of persons to whom a right of access has been granted shall be subject to periodic review. On the basis of this review, access to Personal Data may be revoked if it is no longer necessary, and therefore such persons will no longer be able to access the Personal Data.

4.2 At the request of the Controller, the Processor shall prove that such persons under its supervision are subject to the aforementioned obligation of confidentiality.

4.3 The Processor shall take all reasonable measures to ensure adequate training of its personnel processing Personal Data with regard to compliance with this Annex and applicable legislation on the protection of personal data.

5. Security of processing

5.1 Article 32 GDPR states that, taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure an appropriate level of security against risks. The Controller shall assess the risks posed by the processing to the rights and freedoms of natural persons and shall take measures to mitigate those risks. Depending on the significance of the risks, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure the confidentiality, integrity, availability and reliability of processing systems and services on an ongoing basis;

c. the ability to restore the availability and access to personal data in due time in the event of a physical or technical incident;

d. procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

5.2 With regard to the level of security of the processing to be carried out by the Processor, account should be taken of the fact that the processing involves a large amount of Personal Data, some of which may fall under Article 9 GDPR for 'special categories of personal data', which is why a 'high' level of security should be established.

5.3 The Processor is henceforth entitled and obliged to take decisions on the technical and organisational security measures to be implemented in order to achieve the necessary (and agreed) level of data security. In any case, however, the Processor shall at least apply the following measures agreed with the Controller:

List of key personal data security measures

[the above link of the list is available, which you can enrich with additional measures and attach to this Annex. These additional measures may concern the following categories:

[DESCRIBE THE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE THE REQUIREMENTS FOR ENSURING THE CONFIDENTIALITY, CONTINUITY, AVAILABILITY AND RELIABILITY OF SYSTEMS AND PROCESSING SERVICES ON A CONTINUOUS BASIS]

[DESCRIBE THE REQUIREMENTS FOR RECOVERABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A NATURAL OR TECHNICAL EVENT]

[DESCRIBE THE REQUIREMENTS FOR THE PROCEDURE FOR REGULAR TESTING, ASSESSMENT AND EVALUATION OF THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SAFETY OF PROCESSING]

[DESCRIBE THE REQUIREMENTS FOR INTERNET ACCESS]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS DURING TRANSFER]

[DESCRIBE THE DATA PROTECTION REQUIREMENTS AT STORAGE]

[DESCRIBE THE MATERIAL SECURITY REQUIREMENTS OF THE PLACES WHERE PERSONAL DATA ARE PROCESSED]

[DESCRIBE THE REQUIREMENTS FOR WORK AT HOME/DISTANCE]

[DESCRIBE THE CONNECTION REQUIREMENTS]

5.4 In accordance with Article 32 of the GDPR, the Processor shall also assess — independently of the Controller — the risks posed by the processing to the rights and freedoms of natural persons and take measures to mitigate those risks. To this end, the Controller shall provide the Processor with all information necessary to identify and evaluate these risks.

5.5 In addition, the Processor assists the Controller in ensuring compliance with the Controller's obligations under Article 32 GDPR, including by providing the Controller with information on the technical and organisational measures already implemented by the Processor in accordance with Article 32 GDPR, as well as any other information necessary for the Controller to comply with its obligation under Article 32 GDPR. If subsequently — in the assessment of the Controller — mitigation of the identified risks requires further measures to be taken by the Processor, in addition to those already applied in accordance with Article 32 GDPR, the Controller shall specify those additional measures to be applied by an amendment to this Article.

6. Use of processing subcontractors

6.1 The Processor should meet the requirements set out in Article 28(2) and (4) GDPR in order to recruit another processor (sub-processor).

6.2 The Processor therefore does not employ another processor (sub-processor) to fulfil its obligations under the main contract without the prior specific written permission of the Controller.

6.3 The Processor shall recruit sub-processors only with the specific prior authorisation of the Controller. The Processor shall submit the request for a specific permit at least one month before the sub-processor is recruited. The list of sub-processors already authorised by the Controller is set out in the following paragraph.

[specify time period, indicatively one month]

6.4 Authorised subprocessors

Upon the entry into force of this Annex, the Controller shall authorise the use of the following sub-processors for the processing described in respect of that contractor:

NAME	ADDRESS	DESCRIPTION OF THE PROCESSING

The Processor shall not be entitled to hire a sub-processor for processing other than that agreed, or to have the processing described as carried out by another sub-processor, except under conditions 6.2 and 6.3 hereof.

6.5 Where the Processor employs a sub-processor to carry out specific processing activities on behalf of the Controller, the same data protection obligations set out in this Annex shall be imposed on the sub-processor by means of a contract or other legal act in accordance with national or European law, in particular in order to provide sufficient assurances on the application of appropriate technical and organisational measures to ensure that the processing meets the requirements of this Annex and the GDPR. Consequently, the Processor must (a) before hiring any new sub-processor, carry out a due diligence process to ensure that the sub-processor is capable of ensuring the level of protection of Personal Data provided for in this Annex and the GDPR and (b) ensure that its sub-processors are contractually bound by the same obligations relating to the processing of the Personal Data as those binding the Processor in accordance with this Annex and the GDPR.

6.6 A copy of the sub-processing agreement and subsequent amendments shall be submitted to the Controller upon request to enable the Controller to ensure that the sub-processor is subject to the same data protection obligations as set out in this Annex. Clauses on business matters that do not affect the legal content of the sub-processing agreement with regard to data protection shall not be submitted to the Controller.

6.7 If the sub-processor fails to fulfil its obligations relating to the protection of personal data, the Processor shall remain fully accountable to the Controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR, in particular those provided for in Articles 79 and 82 GDPR, vis-à-vis the Controller and the Processor, including the sub-processor.

7. Place of processing — Transfer of data to third countries

7.1 The processing of personal data under this Annex may not be carried out in locations other than the EU and EEA without the prior written authorisation of the Controller.

7.2 Any transfer of Personal Data by the Processor to third countries, for which the EU has issued an adequacy decision and where the standard contractual clauses are applied, or to international organizations, shall only take place on the basis of recorded instructions from the Controller and always in compliance with Chapter V of the GDPR.

7.3 Therefore, without recorded instructions from the Controller, the Processor cannot, under this Annex:

a. transfer personal data to a controller or processor in a third country or an international organisation;

B. entrust the processing of personal data to a sub-processor in a third country;

c. process personal data itself in a third country.

8. Assistance to the controller

8.1 Taking into account the nature of the processing, the Processor provides assistance to the Controller with appropriate technical and organisational measures, to the extent possible, to fulfil the obligations of the Controller to respond to requests for the exercise of the data subject's rights provided for in the GDPR and in Law 4624/2019. This implies that the Processor provides assistance, to the extent possible, to the Controller to fulfil the rights of data subjects as provided for in Articles 12-22 GDPR.

8.2 In addition to the obligation of the Processor to assist the Controller pursuant to Article 5.4 hereof, the Processor shall also assist the Controller, taking into account the nature of the processing and the information available to the Processor to ensure compliance with:

a. the Controller's obligation to notify without delay and, if possible, within 72 hours of becoming aware of the personal data breach, the personal data breach, unless the personal data breach is unlikely to cause a risk to the rights and freedoms of natural persons;

b. the Controller's obligation to communicate without delay the personal data breach to the data subject where the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons;

c. the obligation of the Controller to carry out, where appropriate, an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment);

d. the obligation of the Controller to consult the competent supervisory authority prior to processing where the data protection impact assessment indicates that the processing would cause a high risk in the absence of risk mitigation measures by the Controller.

8.3 To the extent possible — within the scope and extent of the assistance specified below — the Processor shall assist the Controller in accordance with paragraphs 8.1. and 8.2 above by taking the following technical and organisational measures:

[DESCRIBE THE SCOPE AND EXTENT OF ASSISTANCE TO BE PROVIDED BY THE PROCESSOR]

[DESCRIBE THE SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES TO BE TAKEN BY THE PROCESSOR IN ORDER TO ASSIST THE CONTROLLER]

9. Data breach notification

9.1 In the event of a personal data breach, the Processor shall inform the Controller of the personal data breach without delay from the moment it becomes aware of the breach.

9.2 The Controller's notification by the Processor shall take place without delay and, in any event, within 24 hours after the Processor becomes aware of the personal data breach, in order to enable the Controller to comply with the obligations to notify the personal data breach pursuant to Articles 33 and, where applicable, 34 GDPR.

[More time can be specified than 24 hours but less than 72 hours.]

9.3 In accordance with Article 8(2)(a), the Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority. This means that the Processor is obliged to assist in providing the information listed below, which, pursuant to Article 33(3) GDPR, is reported in the controller's notification to the competent supervisory authority:

a. the nature of the personal data, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records affected;

b. possible consequences of the personal data breach;

c. measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

9.4 If the Processor is unable to provide all the information referred to in paragraph 9.3 within the timeframes provided for, then before the expiry of the above mentioned timeframe, it shall explain to the Controller the reasons for the delay, providing an indication of when it is expected to be able to provide the relevant details (possibly also occasionally), and inform the Controller at regular intervals of these matters.

9.5 Following the detection of the data breach, the Processor will (a) conduct an investigation into the data breach without undue delay and provide information to the Controller about the breach, (b) take reasonable steps to limit the impact and minimise the damage caused by the data breach, including assisting the Controller in remedying or limiting the potential damage from the breach, to the extent that such remedy or restriction is under the control of the Processor, as well as reasonable measures to prevent a recurrence of the data breach and (c) cooperate fully with the Controller to develop and implement an action plan to address the breach.

10. Erasure and return of data

10.1 Personal data are stored for the entire period of validity of the main contract between the parties and then automatically deleted by the processor.

10.2 Upon termination of the provision of personal data processing services, the Processor is obliged, at the choice of the Controller and in accordance with its instructions, either (a) to return all Personal Data to the Controller, or (b) to delete all Personal Data, providing in any case within a specified period of time [indicatively mentioned] of fifteen days after the end of the cooperation written certification to the Controller that the processor and any of its sub-processors no longer keep copies of Personal Data obtained by virtue of the main contract, unless a provision of national or European law requires further storage of the Personal Data.

10.3 In the event that, despite the expiration of this Annex, the applicable law requires the storage of any Personal Data by the Processor, the Processor shall (a) inform the Controller of this requirement, in which case it will become the Controller for such limited purposes, and (b) ensure that the Data is processed only to the extent necessary to comply with the applicable law requiring storage, to the exclusion of any other purpose.

11. Control and inspection

11.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and this Annex and shall permit and facilitate audits, including inspections, carried out by the Controller or by another auditor authorised by the Controller.

The Controller or the representative of the Controller [specify the period of time, indicatively every five months] shall carry out an inspection of the sites where the Processor carries out the processing of the Personal Data, including the physical facilities as well as the systems used and related to the processing in order to verify the Compliance with the GDPR, the applicable data protection provisions and this Annex.

In addition to the scheduled inspection, the Controller may inspect the Processor when it considers that such an inspection is necessary.

11.2 The Processor shall be obliged to grant the supervisory authorities, which under the applicable law have access to the premises of the Controller and the Processor, or to representatives acting on behalf of those supervisory authorities, access to the physical premises of the processor on presentation of appropriate identification documents.

12. Entry into force and expiry

12.1 This Annex shall enter into force on the date of its signature by both parties.

12.3 This Annex shall apply throughout the provision of the services of the main contract by the Processor to the Controller.

12.4 If the provision of personal data processing services expires and the Personal Data is deleted or returned to the Controller in accordance with Article 10 of these presents, either Party may terminate this document by written notice.

5.10 Website requirements on transparency, security measures and cookie compliance

5.10.1 Checklist of clear requirements for a business website regarding transparency

1. Who manages/owns the website (data controller): Name, address, contact details.

2. If there is a Data Protection Officer, his/her contact details.

3. In which cases visitors' data are processed (indicative examples: visitor IP collection, contact form, user registration forms, profile creation).

4. What kind of data is collected: Description of data collected in each case, such as: identification details (name), contact details (e-mail, home address, telephone), transaction details (orders, payment method, invoicing details, cancellations/refunds, etc.).

5. Purpose and legal basis for processing in each case. For example, the purpose of collecting the data in the contact form is electronic communication with the business and the legal basis the consent of the subject (art. 6.1a GDPR).

6. In the case of processing on a legal basis of the overriding legitimate interests of the controller or third party (6.1.f GDPR, e.g. for direct promotion purposes), what are the legitimate interests pursued.

7. Who are recipients or categories of recipients of the data (indicative examples: hosting provider, partners providing technical support, marketing or competition providers).

8. If there is a transfer outside the EU, the legal basis for the transfer (Commission adequacy decision, appropriate safeguards, binding corporate rules or specific derogations under Articles 45-47 or 49(1) GDPR).

9. The period of time for which the data of visitors or users of the website are retained or, if this is not possible, the criteria determining that period.

10. What rights do the data subjects have (Articles 7(3), 15-18 and 21-22 GDPR, depending on the legal basis of the processing, and the right to lodge a complaint with a supervisory authority).

11. How the rights of the data subjects can be exercised.

5.10.2 Checklist of clear requirements for a business website regarding the security measures

Security of communication networks

1. Maintain a comprehensive and up-to-date overall network diagram.
2. Separate the network into critical zones (sub-networks) creating distinct physical networks to separate traffic (e.g. Internal Network – Demilitarised Zone (DMZ) – Perimetric Network – External Network).
3. Prohibit any direct communication between internal workstations and external networks (e.g. use of network address translation to match internal and external IP address and use proxy server and/or firewall for content filtering).
4. Use only connections that are explicitly allowed (limit to the strictly necessary communication ports for the proper execution of installed applications – application of the deny-all rule in addition to the strictly necessary authorized addresses and communication port).
5. Monitor and control network activity through Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS).
6. Keep a log of online requests to investigate them in case of a security incident.
7. Prohibit connection to the computer network and any type of device without prior checking and approval by competent personnel or security officer, if designated.
8. Use web application firewall.

Security of servers, applications and databases

1. Install security updates of the server operating system as well as applications.
2. Protect against malicious software by implementing appropriate certified and up-to-date programs
3. Use secure Internet Channel Encryption Protocols (TLS) when transmitting data over public networks and a certificate of authentication of the server by a trusted third party entity (absolutely necessary in case of electronic transactions).
4. User accounts:
    a. Use of strong passwords for administrators and users.
    b. Use of two factor authentication (at least in the case of exchange of data of an economic nature, e.g. credit card details or data of special categories).
    c. Limitation of administrator connections (administrator access must be justified, authorised and recorded without being able to delete the log by the administrator).
5. Change predefined server error messages.
6. Protect system files and folders (e.g. .ini, .sys, etc.) and parameters (e.g. cfg).
7. Install security software on servers (e.g. Apache mod-sec].
8. Secure configuration of file for the configuration of the server setting.
9. Regular secure backups of servers, applications and files.
10. Non-use of servers used for databases containing personal data for other purposes, in particular for web service or mail servers.
11. Protection against SQL attacks or script injection
    a. Prohibit input of data into web applications by a user that is not of a specific type (e.g. by specifying the format) – filter the data entered by the user.
    b. Prohibit importing large volumes of data (e.g. limiting the size of attachments).
    c. Disable the use of the data entered by the user to perform any tasks (e.g. identifying and rejecting data that may initiate an executable command).
12. Identify security measures in the contract with a processor in case of outsourcing.

5.10.3 Checklist of clear requirements for a business website regarding compliance with cookies

1. What are cookies

Cookies are small files containing information that a website stores on a user's or visitor's computer so that each time it connects to the website it retrieves that information and offers the user related services. A typical example of such information is the user's preferences on a website, as indicated by the choices made on that website (e.g. selecting specific "buttons", searches, ads, etc.).

Article 4(5) of Law 3471/2006 provides that the storage and access to information stored in user terminal equipment shall be permitted only if the subscriber or user has given his or her consent after clear and extensive information.

As an exception to the obligation to obtain consent, Article 4(5) of Law 3471/2006 defines the case of storing and accessing information for the sole purpose of "performing the transmission of a communication over an electronic communications network or necessary for the provision of an information society service explicitly requested by the user or subscriber".

2. Checklist of basic requirements for website compliance with cookies

A. Consent to the use of optional cookies

1. The use of cookies is allowed only with the consent of the user/visitor and after the provision of appropriate information.
2. Excluded are cookies that are considered technically necessary to make the login to the website or to provide the internet service (authentication cookies, session cookies, cookies that "remember" the user's choices).
3. Consent is given with positive action of the user/visitor for each separate category of cookies and not with pre-filled checkboxes.
4. Provision of central management of users' preferences for cookies at all times and in an easy way through the website.

B. Transparency – conditions for informing users/visitors of the website for cookies

1. Information about the use of cookies should be provided in an easily accessible, comprehensible and structured form.
2. A cookie banner should appear containing concise and comprehensive information about cookies, not pre-filled checkboxes for obtaining consent for the different categories of optional cookies and total rejection of all categories of optional cookies
3. Drafting and uploading a cookie policy on the website
4. Minimum content of the cookie policy
    a. Details of the website's owner
    b. Purpose of the cookies policy
    c. Definition of cookies
        - Explanation on first party or third party cookies if used by the website. First-party cookies are those that are installed by the website's provider and third party cookies are those installed by others (e.g. advertising networks) through the provider of the website.
    d. List of categories of mandatory technically necessary cookies and their use purposes
        - Technical cookies are necessary for the website to function properly. They allow users to use the internet services provided, including the management and operation of the website such as a) maintaining the user's connection and content (completing an online form, registering selected products in an "order basket", making the purchase and managing the payment), b) authentication of the user, c) the ability of the website to "remember" the choices that the user himself requests in terms of language, presentation of search results, etc.

e. List of optional categories of cookies and their use purposes such as traffic analysis and measurement cookies, advertising cookies, page sharing cookies on social networks
   - Analysis or measurement cookies collect information on how users interact with the website in order to statistically analyze and improve the use of services provided, product applications and website content.
   - Behavioural advertising cookies store information about browsing habits, behaviour and actions taken by users online (e.g. purchases of products and services), with the aim of displaying advertisements only on the basis of their interests and preferences.

f. Information on the cookies of each category (table with at least the following fields: cookie name, category, purpose of use, retention period, provider)

Cookie name	Category	Purpose of use	Retention period	Provider (first party/third party)

g. Link to information to manage cookies from the browser (Microsoft Edge, Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera)

5. Minimum requirements for the cookie banner of the website
   a. Text of concise and comprehensive information in the cookie banner for the categories of cookies used
   b. Grouping of cookies by category based on the purpose of their use
   c. Ability to reject all optional categories of cookies with one option (with a separate button) at the first level of the cookie banner
   d. Ability to choose each optional category of cookies individually (with positive action) (with separate checkbox) at the first level of the cookie banner
   e. No pre-selected checkboxes for the selection of the optional categories of cookies
   f. Ability to close the cookie banner without selecting any of the optional categories of cookies and installing only the technically necessary cookies
   g. Ability to manage cookies with an option leading to detailed second level information (button “Cookie Settings”) and provide the possibility to change the user’s choices

5.11 Direct marketing through electronic means

5.11.1 Frequently Asked Questions for direct marketing through electronic means

1. Can I send advertising e-mails/sms to my customers?

Yes, if you have their details in the context of a previous transaction and provided that the advertisements relate to similar products and/or services and if your customer was informed during the collection of contact details that his e-mail or mobile phone number will be used to promote products and services and had not objected to the sending of such messages. Then you can advertise similar products, but you should allow the recipient to object in an easy way and to any message to further send such messages.

2. Can I send advertising e-mails/sms to potential new customers, whose details I have

a) from ready-made mailing lists and/or publicly accessible catalogues?

No, unless prior to sending any message you have received their written or electronic consent after informing potential customers. If you use a list of recipients provided to you by a third party (e.g. a sales promotion company), the third party must prove the lawful creation of this list (previous information and consent of the owners of the email addresses contained therein).

It is not lawful to send advertising messages to potential customers when their data are derived from lists of professional associations, unions, clubs, online directory enquiry services.

B) with consent prior to GDPR application?

Consent obtained before the Regulation applies, if it fulfils the conditions, set by the GDPR for the valid obtaining of consent. In practice, you have to review the procedure by which consent was obtained, the information you provided in order to obtain it, the possibility of revoking it proportionately and without hindrance and how to substantiate the above.

3. How can I lawfully obtain the consent of potential customers?

You can obtain the consent of recipients on paper, for example by distributing promotional forms in exhibitions or product presentations.
You can also obtain consent in electronic form, e.g. by using a system in which the recipient’s electronic data is checked (double opt-in or “verified opt-in”). Please refer to the Authority 's Directive 2/2011 on electronic consent.

In any case, you must have previously informed the recipient in the manner mentioned in question 4 below, also providing information about the possibility of subsequently deleting it from your file (or otherwise withdrawing consent).

The consent declaration in any case must be explicit, e.g. the recipient chooses consent; the relevant field should not be pre-selected.

More information about sending a newsletter is available here and about the conditions for using consent as a legal basis for the processing of personal data here.

4. What information should I provide to recipients during the data collection phase?

In any case, and before obtaining the consent, you must inform the recipients of the messages about your identity (e.g. name, address, telephone and e-mail address), the purpose of the data processing, the existence of the right of access, as well as the potential recipients of the data (e.g. third parties cooperating with you).

When informing the recipients of the data, you should indicate specifically those recipients (e.g. company X, Y) or the general professional category of recipients (e.g. electronic sales companies).

More information on providing information to data subjects — transparency is available here.

5. What information should be provided in advertising messages?

The exact identity of the sender-advertiser and a valid way (usually e-mail address) by which the addressee can object to further mailing must be clearly provided.

6. Can I contact potential customers by telephone for advertising purposes?

Yes, if this is a telephone call with human intervention and after you have checked the register referred to in Article 11(2) of Law 3471/2006 which includes telephone subscribers who have declared that they do not wish to receive advertising calls. In the absence of a single register for all telephony providers, you should search and check the relevant up-to-date registers from all providers. At the same time, you should ensure that you have up-to-date files at your disposal each time before making the telephone, ensuring that you have the statements of subscribers made up to thirty days before the call is made.

Moreover, before making the telephone communication you must check your own files (which you keep) and include a) those who, freely and explicitly, declare that they wish to receive advertising calls from you (even if they are included in the above-mentioned register) and b) those who declare that they do not wish to receive advertising calls specifically from you, exercising the right to object under Article 21 of Regulation (EU) 2016/679 even if they are not included in the register.

When making a telephone call, you must inform of your identity and/or the identity of any representative (e.g. company call center), not conceal or falsify the caller number and at least inform about the possibility of exercising the right of access.

7. What measures should be followed to respond to the requests/complaints of the recipients?

- ✓ In the case of sending advertising messages by electronic means, you should give recipients the opportunity to update the personal data you keep in your file, the possibility to exercise the right of access to such data, the right to rectify, upon request, if there are errors in the logs or an update of existing data is sought, as well as the right to erasure.
- ✓ In addition, you should keep the declarations of consent of the recipients in a special file.
- ✓ You must also provide a clear procedure by which the recipient can withdraw his/her consent and request his/her removal from the mailing list. In the same or in a different file as of the consents, you must also keep requests for removal of the recipients, which will record the date of removal of the recipient, as well as the contact details to which your e-mails were sent (e.g. e-mail address).
- ✓ You should also take all necessary technical and organisational measures to ensure the security of the file or to preserve the confidentiality, integrity and availability of the data.
- ✓ Furthermore, it is also advisable to set up a specific and clear procedure for following up and handling complaints for sending unsolicited communications.
- ✓ If the promotion of products and services is outsourced to a third company, it is necessary to have specific clauses on matters relating to compliance with Article 11 of Law 3471/2006 in the relevant contracts. In addition, you must take steps to ensure that the relevant procedures are followed by both your employees and processors, such as through periodic on-the-spot checks.
- ✓ In particular, in the case of telephone communication with human intervention for direct promotion purposes, a specific procedure for making calls and handling requests and complaints should also be followed. In other words, there must be recorded, appropriate procedures and corresponding written instructions must be provided to the employees of the controller and to the staff of any processors (external partners) which, as a minimum, include how the call procedure is carried out, the information the employee is required to report at the time of the call, more detailed information on how the rights of called subscribers can be fulfilled.
- ✓ Also, in case a called subscriber objects to receiving calls from you specifically (and/or by your representative), a clearly defined procedure must be followed, ensuring that this number will be excluded from any future promotional/advertising action. The same process should also be known and respected by external partners. You must keep secure log-files of the information necessary for the

investigation of any complaint, such as external contact details (date and time of call, caller's and call-recipient's numbers). These records must be kept for one year. You should also have a complaint hotline, which you should make public.

8. In what terms can I use the fans/followers data on my Social Media page for direct promotion purposes?

It is only possible if they give their consent with clear action. Users should give their consent to receive promotional emails, having received clear information about the processing of their personal data for advertising purposes, commensurate with the information you have to provide through your website when collecting contact details of potential customers.

Moreover, since the company carrying out advertising activities is considered to be a joint controller with the provider of the relevant social media, the contact point, i.e. whom they can contact for the exercise of their rights, should have been identified and communicated to users, but this does not preclude the possibility of addressing either of them.

5.11.2 Instructions for sending e-newsletters - model information text and template e-mails

1. Legal basis

The collection and maintenance of e-mail addresses for the purposes of direct marketing of products or services and for all kinds of advertising purposes, including the sending of newsletters, is permitted only if the recipient (user) has expressly consented in advance, in accordance with Article 11 of Law 3471/2006. Consent may be given electronically (see Authority Directive 2/2011) and must be given in full knowledge, after appropriate information is provided, and recorded in a secure manner by the Controller.

2. Information

The information to users wishing to subscribe to the newsletter must be distinct from the general information provided by the Controller (e.g. the terms of use of the website) and includes at least the following information: the identity (name or legal name) and contact details of the Controller, the purpose of processing (sending newsletters), the data or categories of data concerned by the processing (e-mail address and any other data collected), the recipients or categories of recipients of the data (e.g. a marketing service provider), including any transfer to a country outside the EU on the appropriate legal basis; the period of time for which the data will be stored, as well as the rights of the user (access to his or her data, rectification if inaccurate or incomplete, withdrawal of consent for the future, deletion of his/her data if the conditions of Article 17 GDPR or restriction of processing under Article 18 GDPR are met and lodging a complaint with the supervisory authority). The relevant information must be provided in an easily and directly accessible way to the user prior to the declaration of consent, such as a pop-up window summarising the above information and a link to a webpage where more detailed information about the processing is provided.

3. Consent procedure

Consent to receive a newsletter is given by filling in an icon at the end of the information text or by filling in the user's e-mail address in a relevant registration form. The Controller should first confirm that the user has access to this address by sending an initial information message to the stated address, which will include a link to the detailed information text for such processing and provide an easy way of withdrawing consent if the user so wishes (consent with additional information). Alternatively, along with the initial confirmation message a link may also be sent to activate the subscription to the newsletter (confirmed consent) within a certain period of time, unless the user's email address has been confirmed as part of his/her registration with another web service of the Controller.

4. Other obligations

Each newsletter sent should include the possibility to withdraw the user's consent, such as a unsubscribe link from the newsletter's mailing list. This option should also be provided by a relevant option in the user area of the website, in the case of registered users. The user who chooses to unsubscribe from receiving newsletters should be informed about the completion of the consent withdrawal process, e.g. by e-mail.

The Controller should be able to satisfy the rights that may be exercised by the data subjects – recipients of newsletters, maintaining in a secure manner all relevant information. In case of exercise of the right to rectification, erasure or restriction of processing, the Controller must communicate it to the recipients to whom the data have been disclosed (such as marketing companies).

5. Duration of keeping declarations of consent

The declaration of consent must be kept for as long as the newsletters are sent to the user and in any case no more than six months after the Controller's promotions have ceased or the user's consent has been withdrawn. Withdrawal of consent must be kept for the same period of time.

6. Security measures

The Controller must take appropriate technical and organisational measures to protect the personal data processed for the above purpose.

List of key personal data security measures

7. Model information text in the registration form

(May be included in a pop-up window or in a text appearing before the form where the e-mail address of the user wishing to register is filled in)

[*Company*] collects your e-mail address based on your consent to send newsletters and promotional material for its products/services. Your data is not shared with third parties. More information can be found here.

8. Templates for confirmation e-mails

A. With additional information

From: newsletter@etaireia.gr

Topic: Registration on the list of recipients of the Company's newsletter.

You receive this message because you, or someone who used your address, was entered on the list of recipients of the Company's newsletter from its website, http://www.etaireia.gr.

We particularly thank you for your registration.
If you have not requested your registration or if you have changed your opinion, you can cancel your registration at any time by clicking on the following link:
http://www.etaireia.gr/newsletter/unvalidate.php?id=ASDWVCHTGHFSDCFSD2DFS5SA
or by visiting http://www.etaireia.gr/newsletter/unvalidate_online.php and entering the code ASDWVCHTGHFSDCFSD2DFS5SA. In this case, your email will be deleted automatically from our list.
The possibility to unsubscribe from our newsletter is also available in each individual message you will receive in the future.
Detailed information at http://www.etaireia.gr/newsletter/subscribe.php

B. With confirmed consent

From: newsletter@etaireia.gr

Topic: Registration on the list of recipients of the Company's newsletter.

You receive this message because you, or someone who used your address, requested registration on the list of recipients of the Company's newsletter from its website, http://www.etaireia.gr. If you have actually requested your registration, you must activate it within a week by clicking on the following link: http://www.etaireia.gr/newsletter/verify.php?id=ASDWVCHTGHFSDCFSD2DFS5SA or by visiting http://www.etaireia.gr/newsletter/verify_online.php and entering the code ASDWVCHTGHFSDCFSD2DFS5SA.
If your registration is not activated within the above timeframe, your email will be deleted automatically from our list.
Detailed information at http://www.etaireia.gr/newsletter/subscribe.php

[*And then, if the registration is activated*:]

From: newsletter@etaireia.gr

Topic: Completion of registration on the list of recipients of the Company's newsletter.

Thank you for registering on the list of recipients of the Company's newsletter.
If you wish to be removed from this list, you can follow the link
at http://www.etaireia.gr/newsletter/unsubscribe.php
This link will be included in each message you receive from our list.

5.12 Video surveillance

5.12.1 Frequently Asked Questions on video surveillance systems

1. Definition of video surveillance system

- What is a video surveillance system?

Video surveillance systems are those systems which are permanently installed in a space and capable of receiving and/or transmitting images and/or sound to projection screens or recording machines (where cameras can be connected to the monitor or recording machine either directly or via a network/internet).

The most common case of such a system is closed-circuit television.

If a video surveillance system receives an image from persons (whether or not the system is in permanent operation), personal data are processed. It should be noted in particular that even the mere taking of images, without recording/storage, also constitutes processing of personal data, so the conditions of lawfulness of the GDPR apply.

- What about fake/virtual cameras/video entry phone system?

Hand-held cameras, photographic cameras, mobile phones and entry phones/video entry phone systems which are activated by the persons coming in and which do not record are not considered video surveillance systems: therefore, the content of this section (video surveillance systems) does not cover photoshooting/video recording carried out with these systems.

Fake cameras don't process personal data. It should be noted, however, that such a closed-circuit television system, although not functioning, may make citizens believe that personal data are being processed. Such a belief may affect the citizens' conduct, so the setup of such a system may infringe the constitutionally guaranteed right to the free development of one's personality (Article 5(1) of the Constitution).

2. Purposes for which the use of a video-surveillance system is permitted;

- For what purposes is video surveillance allowed and on what legal basis?

Under the Authority's Directive 1/2011, which regulates the use of video surveillance systems for the protection of persons and property, the objectives are divided into:

- **protection of persons and property**, which may be pursued by all types of public bodies or natural or legal persons in premises they manage.
- **provision of health services**, which is essentially a particular case of the protection of persons, and controllers can only be natural or legal persons active in the field of health and are bound by specific professional secrecy — e.g. doctors, nursing staff.

The legal basis for the above purposes is the legitimate interest pursued by the controller or a third party, unless such interests do not prevail over the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child (Article 6(1)(f) GDPR).

For purposes other than the protection of persons and goods, which fall within the scope of the GDPR, controllers have to follow the general approach to assess the lawfulness of a processing, with a choice of an appropriate legal basis, compliance with the basic principles of lawfulness, consideration of data subjects' rights, etc. The lawfulness of such processings is judged by the controller on a case-by-case basis and properly documented with the GDPR accountability tools.

Following the entry into force of Regulation (EU) 2016/679 (GDPR) and Law 4624/2019, this Directive (as well as the relevant decisions and opinions of the Authority) applies in conjunction with the new provisions of the GDPR.

- Is video surveillance systems allowed to monitor employees?

The operation of video-surveillance systems for purposes such as monitoring employees for their inspection/evaluation or training purposes is not allowed (see in this regard Article 27 of Law 4624/2019, as well as Article 7 of Directive 1/2011).

- Is it allowed to use web cameras to view images on websites for advertising purposes — conditions?

In order to advertise a place or business, it is not necessary to use images where persons are identifiable. You should:

- either put the cameras in such a way that it is not possible to identify persons or car plate numbers (in which case personal data are not processed);
- or take appropriate measures, such as blurring techniques, if the image always includes faces, so that they are not identifiable. In this case, personal data are processed.

In addition, the displayed image should not identify persons and/or car plates, as personal data are processed unlawfully (unless you have the explicit consent of all the data you process, which is impracticable in most cases).

3. Conditions for installation and operation of a system

The following are not allowed:

- the taking of images in places where the hard core of the right to privacy is violated, such as toilet rooms and lobby rooms, changing rooms and staff/customer baths, etc.
- the use of zoom cameras, except under very specific and special conditions.
- the operation of cameras in catering and leisure venues, in changing rooms, and in premises where employees of the store work and are not accessible to the public
- supervision in workplaces (for example, in a typical office space, office or corridor supervision is not allowed). An exception may be specific critical sites (e.g. high-risk facilities, banks, military factories) as long as cameras focus on the good they protect. In any case, data collected by a video surveillance system may not be used for employee evaluation.
- recording sound, except in very exceptional cases
- the taking of images from side roads and/or pavements, or from entrances or interiors of neighbouring dwellings or buildings or other premises
- the placement of cameras in a public place by an individual for the purpose of protecting persons and property. In exceptional cases, such a recording may be permitted only in the case of an area with increased security needs identified (a) either because of the 'nature' of the site (e.g. state buildings, large hotels) (b) or because it is an area where dangerous attacks on life and property have occurred and there are now justified grounds for suspecting that others may take place (e.g. automatic banking machines — ATM, hotel entry-exit facilities). In such cases the recording must be limited to the strictly necessary side space (e.g. the installation of cameras at ATMs shall be carried out in such a way that only the installation of the machine and the location of the user can be viewed).

- What are the technical **characteristics** that cameras should have (blurring, mask, etc.)?

Privacy-friendly technologies should be chosen, such as systems that can encrypt stored images and/or 'cloak'. When selecting, the aim is to minimise data based on the selection of specific technologies (privacy by design).

4. Retention period

- For how long can I keep the data recorded by the video surveillance system?

The data must be kept for the strictly necessary time — the controller must be able to substantiate the reasons for choosing a specific retention time as strictly necessary. The Data Protection Authority, by Directive 1/2011, set a reasonable maximum period of 15 days, in principle, with exceptions (for banks and financial institutions 45 days, while for credit card and personal identifiers printing companies, data recorded exclusively from the premises where the printing and sending of credit cards and related codes take place is allowed for up to 90 days). Especially for multi-apartment buildings, data must be kept up to a maximum of 48 hours, and for school complexes, etc. until the next working day.

- Can data be retained as an exception to the retention period if legal claims are raised?

The retention time may be extended if an incident occurs and the material can be used as evidence or if a data subject's right to restrict processing is exercised.

5. Information of data subjects

Information on the obligation to inform data subjects about the processing of personal data by means of a video surveillance system.

6. Data subjects' rights

- Does the subject have rights in relation to the processing of his or her data and how can he/she exercise them?

Everyone has the right to access the data of a video surveillance system concerning him/her as a data subject (see Article 15 GDPR). This means that they can request at any time to obtain any information related to the processing (purposes, what kind of data is collected, recipients or categories of recipients, data retention period, etc.), as well as to apply to the controller to have a copy of a piece of video material on which they are depicted or a series of corresponding printed images: if both parties also agree, a simple display of the snapshots will be sufficient.

Accordingly, anyone can object to the processing (Article 21 GDPR), ask for erasure of data (Article 17 GDPR), or 'restriction' of processing (Article 18 GDPR). Such requests should be justified, i.e. the reasons for which the subject considers the processing to be unlawful should be set out. In all cases, the controller must respond without delay and, in any case within one month of receipt of the request (Article 12(3) GDPR): if they do not reply or if their reply is unsatisfactory, then the applicant may make a complaint to the Authority.

7. Transfer of data

- Who can be provided with a video-recorded extract of the video-surveillance system material?

Where a video-surveillance system records a crime in which one is involved as a victim or perpetrator, the latter may request the system operator to provide him/her with the relevant video section of data.

Important notice: Any other use of the recorded material, other than its transmission to the competent authorities (e.g. Police, Courts), in the event of an incident, entails the application of the legislation on personal data and is in principle not allowed.

8. Company located in an apartment building or detached house

- I have a business space in an apartment building. Can I put a camera that overlooks the space in front of my front door?

Cameras can be placed in such a way so that they monitor the interior of your apartment (without, however, overlooking outside your business premises — e.g. no camera is allowed on the balcony which overlooks a public street or the entrance of your apartment building).

A camera can be installed to overlook the absolutely necessary space of your entrance, without image or sound recording (e.g. to see who rings the bell).

A camera with image recording (no audio) can be installed when it is technically possible to limit the scope of the camera to the absolutely necessary space in front of the entrance door of your apartment, without in any case affecting other appartments. In this case:

- No image shall be taken from other public areas; and
- depending on the location of the entrances to the floors and lifts, the entrance to or transit to other apartments must not be affected (at least incidentally).

- I have a business space in a detached house. Can I install cameras for security purposes and under what conditions?

It is allowed provided that no image is taken from an external public space (e.g. road or pavement), as well as from neighbouring buildings (see also Article 3 of Directive 1/2011), and of course fulfil all other obligations.

9. Sector-specific issues

a) Health sector

- Under what conditions is it permitted to place cameras in areas where health services are provided?

In the case of hospitals, clinics, doctors' private offices, diagnostic centres and other areas where health services are provided, cameras may be installed for the protection of persons and property exclusively at entry and exit points, in the premises of treasuries or critical facilities (e.g. electromechanical installations, storage facilities for medical supplies, etc.) where, in principle, visitors or patients cannot have access. Cameras may not in any event check movement in the living rooms, canteens and catering areas, hospital corridors, patient chambers, examination rooms or surgeries, toilets and baths, doctors' offices and the workplaces of other medical and nursing staff.

Furthermore, if it is necessary to install cameras for the purpose of providing health services (e.g. surveillance of serious mental or mentally ill patients that may cause damage to their health or to third parties), then more specific conditions described in the other paragraphs of Article 20 of the Directive must be met (see Article 20(2)(b)-(g) — i.e. only the condition of obtaining a processing authorisation by the Authority is excluded — see Decision 46/2018).

- Is it allowed to operate the system within the patient chambers, operating rooms, etc?

Movement control in waiting areas, corridors, patient chambers, examination booths or surgeries shall not be permitted.

- I have a private practice in an apartment building. Where can I place cameras for security purposes and where not?

You can place cameras that take pictures within your practice but you cannot place cameras externally (e.g. to overlook the hallway or the entrance of the apartment building), because only the manager of the building (e.g. the General Assembly) is responsible for installing cameras at these points and the provisions of Article 15 of the Directive apply. You can place a camera that overlooks the absolutely necessary space of your entrance, without image or sound recording (e.g. to see who rings the bell).

You can place a camera with image recording (no audio) when it is technically possible to limit the scope of the camera to the absolutely necessary space in front of the entrance door of your apartment, without in any case affecting other appartments. In this case:

a. No image shall be taken from other public areas; and

b. depending on the location of the entrances to the floors and lifts, the entrance to or transit to other apartments must not be affected (at least incidentally).

Please note that you are not allowed to have a camera in the lounge/waiting room (see also Article 20 of Directive 1/2011). A camera can be installed, for example, inside the entrance to the clinic room.

b) Tourism-hospitality sector

- In which areas in hotel units are video surveillance systems allowed to operate?

The operation of video surveillance systems in hotel units in any form (hotels, guest houses, rented rooms, etc.) must be limited exclusively to areas intended to control incoming/outgoing persons (such as the central entrance, reception area, entrances/exits of lifts and stairs) as well as in the storage areas (e.g. treasuries) and electromechanical installations. No cameras may be installed in the catering areas and corridors leading to the hotel's rooms and places where guests and/or visitors of the hotel may be monitored. Such spaces include, in particular, entrances to individual rooms, toilets and places where leisure activities take place (such as swimming pools, gyms, sports areas, changing rooms, etc.).

c) Education sector

- Under what conditions is it allowed to place cameras in schools/spaces where minors are present?

The installation of a video-surveillance system in schools and, accordingly, in all other areas of minor activity must be carried out with particular care and under very strict conditions. The decision must be taken by the body responsible for the administration of the school, taking into account the opinion of representatives of teaching staff, parents' associations and pupil associations. The system is not allowed to operate at hours when the school is in operation and everyone (pupils and representatives of the educational community) must be fully aware of it so that they know that they are not being monitored. The data must be deleted on the next working day (if there has been no incident) and in any case its function must be regularly assessed (not longer than one year), and pupils, parents, teachers and other employees must be able to access the information on evaluation (see also Article 18 of Directive 1/2011).

Especially in cases of large-scale school facilities of non-public schools, when it is not practical to control the remote points of the facilities by softer means (e.g. guards), it may be legitimate to operate cameras focusing on remote locations and during school opening hours, but with appropriate safeguards, as resulting from the GDPR.

d) Commercial sector (physical/electronic)

- I own a shop. Where can I place cameras and where not?

Cameras may be placed at the entry and exit points of the premises, in the treasuries and storage areas of money, in the warehouses of goods, in the premises of electromechanical installations and in the stationing areas, under the conditions laid down in the general part of this Directive.

The installation of cameras in the premises of the shops where customers circulate and transactions are carried out may exceptionally be authorised provided that (a) these are large-scale shops (e.g. commercial centres) and (b) the goods are of great value (e.g. jewelry shops). Surveillance must not be ensured in any other way. In such cases, the angle of reception of the cameras should be such as to focus as little as possible on the faces of customers and employees and have as wide a view as possible.

In any case, the operation of cameras in restaurant and leisure venues, in changing rooms, in toilets and in the premises where employees of the store work and are not accessible to the public is not allowed.

If the store is located indoors or on a building floor, the conditions for residential or office complexes shall also apply as far as cameras focusing on public areas are concerned.

5.12.2 Checklist of clear requirements for installing and operating a video surveillance system

☐ Displaying information plates in a sufficient number with appropriate content

Provision of first and second level information based on the Authority's templates

☐ Camera range:

No image capture from sideways and/or sidewalks.

No image capture from entrances or interiors of neighbouring dwellings or buildings or other premises.

No image capture from premises such as toilets and lobby rooms, dressing rooms, changing rooms and staff/customer baths.

☐ Privacy-friendly data protection techniques, such as blurring, mask, ability to encrypt stored images

☐ Sound recording is not allowed.

☐ The use of zoom cameras is only allowed under very specific and special conditions

☐ Retention time: up to 15 days in principle, except for exceptions, as provided for in the case of financial institutions or credit card printing companies and personal identifiers

☐ Specific conditions for the placement of cameras, by processing sector

Health sector:

- only at entry-exit points
- in cash and money storage facilities

it is not permitted:

- in waiting rooms, canteens

- in the corridors
- in patient rooms and examination or medical interventions chambers
- in doctors' offices [more specific conditions apply if it is necessary to install cameras for patient surveillance]

Tourism-Hospitality sector:

- only at entry-exit points of the unit; and
- lifts; and
- stairway enclosures,
- in the reception area,
- in cash and money storage facilities; and
- electromechanical installations,

it is not permitted:

- in the catering areas
- in the corridors leading to the rooms
- in places where customers and/or visitors of the unit may be monitored (pools, gyms, sports areas, changing rooms, etc.)

Education sector:

For the public schools the controller is the municipality where the school is located, which takes the decision after obtaining the agreement of

representatives of the teaching staff

parents' associations, and

students' associations

- for private schools the decision is taken by the school administration, with the agreement of
  - representatives of the teaching staff
  - parents' associations, and
  - students' associations
- similar application to other areas where minors operate
- only during hours when school/equivalent space is not in operation, knowingly of minors
- Retention time: until the following working day

Commercial sector:

- only at the entry and exit points of shops;
- at the cash desks and
- in the places where money is kept,
- in warehouses,
- in the areas of electromechanical installations

☐ apartment blocks

camera with image recording only when it is technically possible to limit its range

- in the space in front of the entrance door of the apartment,

without:

- reception of images from public areas; and
- entrances to or transit to other compartments

Retention time: up to 48 hours

☐ Transfer of data

1. To the data subject; image/video extract depicting him/her (right of access)
2. To the victim and/or perpetrator depicted in the event of a crime
3. Competent authorities

☐ Workplaces with employees:

1. not in standard office space and corridors
2. only over the cash desk
3. in specific critical sites, such as high risk installations, electromechanical installations.

5.13 Management of employee records and prospective employee records

5.13.1 Frequently Asked Questions on the processing of employees' data

1. What personal data of the employee are processed?

The personal data of the employee collected and processed by the Company are:

- ✓ Identification details, i.e. name, father's name and mother's name, ID number, TIN number and tax office, social security number, gender, nationality, date and place of birth
- ✓ Contact details, postal and e-mail address, telephone number (landline, mobile)
- ✓ Individual, family, property and service status of employee and data of dependents (name and date of birth) to the extent necessary for the fulfilment of the company's statutory obligations towards the employee, such as granting of leave, payment of any allowances, processing of wages and insurance obligations.
- ✓ Data on the employee's professional skills and qualifications, as well as his/her professional progress in the company, i.e. curriculum vitae, copies of diplomas, background data, professional certifications, professional licenses, registration number, certificate of fulfilment of military obligations, letters of recommendation and attestations of previous employers, evaluations, productivity bonuses, promotions, trainings, educational permits, criminal record (where required), date of commencement of employment.
- ✓ Data relating to the health of the employee, in so far as they are a precondition for the fulfilment of the company's legal obligations vis-à-vis him/her under labor law, social security and social protection law

and/or other specific laws, such as sick leave or other special-purpose leave and/or necessary to protect and safeguard the health and safety of employees in the company's working environment.

- ✓ Social security data of the employee, i.e. notification to the insurance body (EFKA), notification of recruitment to Manpower Employment Organization (OAED) (where required), retirements, copies of certificates concerning your compulsory insurance.
- ✓ Bank account (Bank and IBAN) for crediting employees' wages.
- ✓ Access data of the employee to the Company's computer network and databases, as well as to the internet from fixed and/or portable electronic devices of the Company (e.g. laptops, mobile phones, tablets), and/or data stored in them, in accordance with the Company's policy/regulation for the use of its electronic means.
- ✓ Photographs and videos of audiovisual material concerning the employee, in the context of social events and/or promotional activities of the Company.

2. What is the purpose of processing and on what legal basis?

The purposes of the processing of the employee's personal data by the employer are the performance of the employment contract, the keeping of a register and individual records of employees, the execution of the payroll, any promotion of the company in the context of social events and/or promotions and any additional benefits to the employee. Accordingly, the legal bases corresponding to the above objectives are the performance of the contract, the legal obligation of the Company, as well as the consent obtained by the Company from the employee for the purposes of promoting the enterprise and any additional benefits to the employee.

3. How long is the data kept?

The employee's personal data are kept by the employer for as long as he/she retains the status of employee in the Company, and after termination for any reason of his/her employment relationship with the Company, for the period provided for under specific legislation or on the basis of criteria determining the period of compliance, such as the expiry of the limitation period of the claims concerned.

If, by the end of the above periods of time, judicial proceedings are ongoing, involving the Company and involving the employee directly or indirectly, the time for keeping the data relating to the employee shall be extended until a final judgment is delivered.

After the expiry of the above time intervals, personal data relating to the employee will be erased/destroyed on the basis of the Company's destruction policy.

4. To whom are the employees' personal data transmitted?

In order for the Company to fulfil its functions and obligations, it communicates the employee's personal data to categories of persons or bodies (recipients), who have access only to those personal data of the employee that are strictly necessary for the performance of their duties or the provision of the services they have undertaken towards the Company.

The categories of recipients are the following:

- ✓ Processors with whom the company cooperates to assist it in fulfilling its legal or contractual obligations, provided that the data of employees are kept confidential, such as:

- accounting service providers
- providers of IT support services
- hosting service providers, cloud providers
- providers of product and promotion services
- physical security service providers

✓ Financial institutions

✓ Tax authorities, social security institutions, health bodies (e.g. National Public Health Organization), if provided for by law.

✓ Lawyers, in so far as this is necessary for the operation of the contract, the performance of the company's statutory or contractual obligations or for the exercise of its rights and the protection of its legitimate interests

✓ Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

Co-operating insurance companies, for the inclusion of the employee in the collective insurance policy of the company, provided that the company provides such additional benefit to the employee.

5. What are the rights of employees and how are they exercised?

The following table shows the employee's rights per processing purpose and corresponding legal basis. By selecting the corresponding right from the table below, the employee will find detailed information (concept, method and time limits for exercise) and a form for exercising it. General information on the exercise of your rights is available here.

PURPOSE	LEGAL BASIS	RIGHTS
Performance of the employment contract	Performance of contract (6.1.b GDPR)	Access 15) Rectification(16) Erasure (17) Restriction (18) Portability (20)
Keeping a register and individual employee records	Compliance with a legal obligation (No 6.1c and 9.2b for special categories)	Access (15) Rectification (16) Restriction (18)
Execution of payroll	Compliance with a legal obligation (No 6.1c)	Access (15) Rectification (16) Restriction (18)
Promotion of the company with photographs and videos depicting employees (on the website, in brochures, etc.)	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17)

		Restriction (18) Portability (20)
Voluntary benefits to employees such as inclusion in a group insurance scheme	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

If the employee wishes to exercise a right, he/she must write to the company's postal address or electronically by sending an email to the Company's email address, using his/her corporate email.

In the case of sending a request document, a copy of the ID, passport or any other document certifying the applicant's identity, certified by a Citizens Service Centre (KEP) or a police authority, should be attached for the purpose of checking the identity of the applicant.

The Company must respond to the employee's request within one month of receipt. This period may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform the employee within one month of receipt of the extension in question and of the reasons for the delay.

If the company does not act on the employee's request in the exercise of the above rights, or following its reply, the employee considers that the above mentioned rights have been infringed, he/she may lodge a complaint with the supervisory authority. The competent supervisory authority for Greece is the Data Protection Authority, Kifissias 1-3, 115 23, Athens, https://www.dpa.gr/, tel. 2106475600.

5.13.2 Frequently Asked Questions for processing of prospective employees' data

1. What personal data of the prospective employee are processed?

The data strictly necessary to achieve the purpose of the processing are collected, such as the following and/or any other data if there is a legitimate purpose and legal basis for processing and the data are strictly necessary for this purpose.

- ✓ Identification details, i.e. first name, father's name and mother's name, ID number, gender, date and place of birth, nationality
- ✓ Contact details, i.e. postal and e-mail address, telephone number (landline, mobile)
- ✓ Marital status, education, curriculum vitae, any disability
- ✓ Background data, professional experience
- ✓ Ground for refusal of a recruitment application

2. What is the purpose of processing and what is the legal basis?

- ✓ The assessment of potential employees as to whether they meet the conditions for recruitment for a specific job. The legal basis for collecting this data is to serve the prospective employer's **legitimate interest** in recruiting qualified and appropriate staff.
- ✓ Information on the possibility of recruitment in future jobs within the company. The legal basis for the prospective employer to collect this data is the **consent** of the prospective employee.

3. How long is the data kept?

- ✓ The personal data of prospective employees who will not enter into a contract of employment shall be retained for six months after the position for which they were collected is filled and they are subsequently deleted.
- ✓ The data of the prospective employees shall be retained for a longer period of up to two years, provided that the prospective employee has given his or her consent and is subsequently deleted.
- ✓ If the prospective employees wish that their data be kept for possible future job opportunities, they can choose for how long, up to two years, and then they are deleted.

4. To whom are the personal data of the prospective employees transferred?

In order for the Company to fulfil its processing purposes and its legal obligations, it communicates the personal data relating to prospective employees to categories of persons or bodies (recipients). The recipients have access only to those personal data that are strictly necessary for the performance of the tasks and the provision of the services they have undertaken vis-à-vis the Company. These categories are as follows:

- ✓ Processors: the Company cooperates with processors on its behalf to provide IT hosting or support services, subject to data confidentiality
- ✓ Lawyers, in so far as this is necessary for the fulfilment of the Company's statutory obligations or for the exercise of its rights and the protection of its legitimate interests
- ✓ Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

5. What are the rights of prospective employees and how they are exercised?

The following table shows the employee's rights per processing purpose and corresponding legal basis. By selecting the corresponding right from the table below, the candidate employee will find detailed information (concept, method and time limits for exercise) and a form for exercising it. General information on the exercise of your rights is available here.

PURPOSE	LEGAL BASIS	RIGHTS
Assessment of potential employees as to whether they meet the conditions for recruitment for a specific job	Serving the legitimate interest of the prospective employer in the recruitment of appropriate staff (6.1f)	Access (15) Rectification (16) Erasure (17) Restriction (18) Objection (21)
Informing the candidate of job opportunities in the Company	Consent (6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

If the prospective employee wishes to exercise a right, he/she must write or electronically send an e-mail to the Company. In any case, for the verification of identity, a copy of the ID, passport or any other authentication document certified by a Citizens Service Centre (KEP) or a police authority should be attached.

The Company must reply to the request within one month of its receipt. This period may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company must inform within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on the request in the exercise of the above rights or, following its reply, the prospective employee considers that his/her rights have been violated, he or she shall have the opportunity to lodge a complaint with the Personal Data Protection Authority, as well as to bring a judicial remedy**.**

6. When is consent required to process the data of the prospective employees?

- ✓ In the case of a retention period of more than 6 months in order to inform the candidate about possible employment opportunities in the Company in the future.

5.13.3 A template of a Use of Electronic Media Policy by employees

A. Purpose

The purpose of this Policy is to lay down the rules for the permissible and correct use of the electronic means of communication provided by the company under the name.....[104] (and distinctive title[105].....), established in..... (street.....no. ..... tel..... e-

[104] Complete full legal name or name in case of sole proprietorship.
[105] Fill in the distinctive title (trade name) of the company, if any.

mail..... (hereinafter referred to as “Company”) to its employees, and the conditions, procedures and guarantees for exercising control over these means and the content thereof.

The company must inform its employees of the application of this Regulation in any appropriate and clear manner so that they are demonstrably aware, at the time of recruitment or commencement of cooperation with the company, their obligations and duties, as well as the rights derived from it.

For the implementation of this Policy, the Company has taken into account the applicable legal and regulatory framework for the processing of personal data and for matters relating to teleworking, as well as the Decisions and Guidelines of the Data Protection Authority.

B. Definitions

For the purposes of this Policy:

Employees: employees with any employment or cooperation relationship with the Company, the concept of which includes the provision of the agreed work or project or cooperation of any kind.

Electronic means of communication' (or 'the means'): Means belonging to the property of the Company and are provided or made available to employees for the fulfilment of their duties and obligations, such as, but not limited to, the provision of access to and use of the Internet, any kind of corporate network and servers, any kind of communication and data storage media, whether personal or not, (e.g. USB sticks, portable disks), all kinds of hardware and software computing infrastructure systems including computer systems, printers, fax machines, modems, communication equipment of any kind, such as mobile phones, laptops and tablets**,** corporate e-mail accounts and use of corporate e-mail, as well as any file containing personal or non-personal data of any kind.

I. Acceptable use of electronic means policy

1. Electronic means of communication, owned by the employer and forming part of the assets of the company, shall be provided or made available to the majority of the employees exclusively for the fulfilment of their duties and obligations, as well as for the achievement of corporate purposes. The above means may not be used for private and other purposes other than the above.
2. The Company provides employees, solely for personal use, with the possibility of using digital storage space, which will be classified as “personal”, provided that the performance and fulfilment of the employee’s duties and obligations are not hindered and the applicable legislation is not infringed.
3. The connection, access and browsing of the internet, as well as the use of corporate e-mail and corporate e-mail addresses attributed to each employee, is permitted exclusively for the fulfilment of his/her duties and obligations, as well as the achievement of corporate purposes.
4. Employees when logging in, accessing and browsing the internet or using corporate e-mail and corporate e-mail address shall refrain from any abusive, unlawful or contrary to their obligations and duties act.
5. An act is regarded as abusive when it technically and substantially burdens the Company’s network**.**

In any case, employees may not, for example:

- **i.** install software programs;
- **ii.** block, remove or circumvent any Internet security means or devices intended to protect the network and business data from viruses and hackers;

iii. distribute e-mails of an offensive, violent, defamatory or slanderous nature, particularly to competitors, customers, suppliers or other employees of the company. Therefore, computing units may not be used to access, process and distribute material containing racist, pornographic or any other illegal, unacceptable and harmful content;
iv. visit websites of illegal content and online gambling;
v. disclose passwords to third parties;
vi. gain access to another employee – colleague's computer without demonstrably explicit consent;
vii. use the software provided to them to attempt to access information and systems for which they have not received the necessary authorization;
viii. 'open' executable files from external storage media connected to users' computing units if they do not comply with the security measures taken by the company;
ix. use the software provided to them for the transfer of data and, more generally, data that are an asset of the company outside the boundaries of the company and outside its systems, without the prior approval of the Head of the department to which they belong.

Employees are responsible for the proper use of their electronic means of communication. It is recommended that devices be switched off when leaving the workplace after the end of the working day.

Accordingly, the Company is obliged to take appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, **unauthorized** dissemination or access and any other form of unlawful processing, such as, but not limited to, the use of encryption software or password to prevent third parties entering the data stored on the computer.

Corporate email

In the event of the departure or dismissal of any employee, the Company will be able to "deviate" the professional email of the former employee for a specified period of time with a specific reference to the departure of the same person, in order to receive any email related to the employee's work for the safe and effective continuation of the work of the business. For this purpose, employees are required not to use professional emails for purposes other than those intended by the Company. The exchange of personal information and data through corporate emails is in no way a good practice of corporate means' use and the company bears no responsibility for any loss, leakage, disclosure, etc. of such employee data**.**

Consequences of non-compliance with the acceptable use policy

In the event of non-compliance by the employee with the above, the competent official (...) shall take the following steps:

1) A recommendation is made to the employee
2) In the event of non-compliance by the employee or a repetition of the incident, a recommendation shall be made to his/her superior.
3) If the non-compliance is repeated, a recommendation shall be made to a Director [if any] and the administration of the company shall be informed [amend accordingly]

II. Policy for access and control of electronic means of communication by the Company

1. Right of control

1.1. The company may collect and process personal data using control methods relating in particular to:

a) the use of electronic means of communication taking place at or in connection with the provision of the agreed work, including any communication, as well as stored personal or non-personal data;

b) the use of corporate e-mail used by the employee;

c) the use of the internet made by the employee.

2. Audit purposes

2.1. The Company shall have the right to carry out the above internal corporate audits, subject to the Acceptable Use Policy of Electronic Communications with a view to satisfying the legitimate interest it pursues and provided that it obviously takes precedence over the rights and interests of the employee without prejudice to the fundamental freedoms of the employee under Article 6(1)(f) of the General Data Protection Regulation (GDPR) and in accordance with the decisions, instructions and opinions of the Personal Data Protection Authority. An audit may be carried out indicatively for:

- ensuring the safe operation of the Company's communication systems;
- compliance with the obligations and duties of employees, the protection of the company and its assets, and its proper functioning;
- compliance with legislation as well as internal corporate policies;
- preventing or deterring unlawful acts and offences;
- the confirmation, proof and verification of unlawful acts or acts committed in breach of internal corporate policies**.**

Audits should be carried out in accordance with applicable laws, including those on the protection of personal data and labor law, if:

- there is no other less onerous control measure that is equally effective
- it is established that there are reasonable indications or elements which make the inspection imperative and necessary (e.g. suspicion of an offence)
- the audit is limited to what is strictly necessary for its purposes, such as persons, records and, in general, electronic means of communication.

The Company reserves the right to inspect the stored data on the employee's computer and stored on the server (except data relating to the personal storage space provided by the company) or the corporate e-mail he/she uses, as well as the use of the internet, in order to protect its legitimate interests.

3. Audit procedure

3.1. In the absence of the exceptions set out below, the employee shall be informed in writing of the purpose, reason and extent of the audit in the records and electronic means of communication concerning him or her so that he or she may be present during the audit.

3.2. The audit shall be carried out by officials designated for this action using tools and software to ensure the security of processing and audit.

3.3. By way of exception, an audit in the records and electronic means of communication without prior information to the employee and/or without his/her presence in the specific case may be carried out if there are compelling reasons of force majeure which make it necessary to check without delay, if the company has to

comply directly with a legal obligation or following a judicial or prosecutorial order or decision or in the context of an investigation or preliminary investigation procedure following compliance with the relevant legislation.
3.4. The company shall, for reasons of security and objectivity of the audit procedure, create a digital or other secure copy of the file found or the images of the electronic means of communication, of which it shall inform the employee at the end of the audit.
3.5. If an audit is carried out without the employee's presence as above, he/she shall be informed of the findings and conclusions of the audit as soon as possible.

Termination of the employment relationship

After termination of the employee's employment relationship with the Company, the employee may, in the presence of a representative of the company, copy on his/her own medium the files entered in the indicated 'personal file' on the company's computer, server, and deleting them at the same time.
It is forbidden to copy or extract in any way other data, personal or otherwise, from the space used on the server or other systems of the company.

When leaving the Company (voluntarily or not), the employee must return in good condition all the equipment he/she has received, as well as deliver any company information/document.

After the departure of the employee, the Company has full access to the employee's computer, including messages, files, documents, fax, communications, as well as to any other storage medium, server, etc. other than the "personal file", which must have already been deleted by the employee himself/herself in accordance with the above.

5.13.4 A template Appendix to the employee employment contract for processing of personal data

ANNEX TO THE CONTRACT WITH AN EMPLOYEE
FOR THE COLLECTION AND PROCESSING OF PERSONAL DATA
(ANNEX TO THE EMPLOYMENT CONTRACT)

In Athens today, between the parties:

on the one hand, the company with the name.....[106] (and distinctive title[107].....), established in..... (street..... no. ..... tel..... e-mail ..... and legally represented by..... (hereinafter referred to as "Company") and

on the other hand ..... residing at ..... with Tax Identity Number ..... tax office ..... and ID number..... (hereinafter referred to as "employee")

Whereas:

(a) The parties have signed the contract of ..... [*date*] (hereinafter referred to as "the main contract"), to which this forms an Annex.

[106] Complete full legal name or name in case of sole proprietorship.
[107] Fill in the distinctive title (trade name) of the company, if any.

(b) The Company collects and processes information relating to the employee and related to the provision of his/her work, which is personal data (hereinafter "personal data" or "data") and as the controller decides the purposes and means of their processing.

(c) With effect from 25 May 2018, 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 "Regulation") and in accordance with the relevant provisions of Greek legislation on the protection of personal data, as in force, has been implemented,

recognize, agree and mutually accept the following:

A. Preamble

This Annex sets out the rights and obligations of the Company, as well as of the employee when processing personal data on behalf of the Company. The Contracting Parties agree to the terms of this Annex in order to meet the requirements of the legislation on the protection of personal data and to ensure the protection of employees' rights as data subjects.

The terms of this Agreement shall take precedence over any similar provisions contained in other agreements between the Parties.

B. Data type and source

The personal data of the employee collected and processed by the Company are[108]:

1. Identification details, i.e. name, father's name and mother's name, ID number, TIN number and tax office, social security number, gender, nationality, date and place of birth

2. Contact details, postal and e-mail address, telephone number (landline, mobile)

3. Individual, family and service status of an employee and data of dependents (name and date of birth) to the extent necessary to fulfil the company's statutory obligations towards the employee, such as granting of leave, payment of any allowances, processing of salaries and insurance obligations.

4. Data on the employee's professional skills and qualifications, as well as his/her professional progress in the company, i.e. curriculum vitae, copies of diplomas, background data, professional certifications, professional licenses, registration number in professional registers, certificate of fulfilment of military obligations, letters of recommendation and attestations of previous employers, evaluations, productivity bonuses, promotions, trainings, educational permits, criminal record (where required)[109], date of commencement of employment.

5. Data relating to the health of the employee, in so far as they are a precondition for the fulfilment of the company's legal obligations vis-à-vis him/her under labor law, social security and social protection law and/or other specific laws, such as sick leave or other special-purpose leave and/or necessary to protect and safeguard the health and safety of employees in the company's working environment.

[108] The reported information is given indicatively and each company should check what is applicable to it.
[109] Each company should request and keep a copy of a criminal record only if it is expressly required by law.

6. Social security data of the employee, i.e. notification to the insurance body (EFKA), notification of recruitment to Manpower Employment Organization (OAED) (where required), retirements, copies of certificates concerning your compulsory insurance.

7. Bank account (Bank and IBAN) for crediting the employees' wages.

8. Access data of the employee to the Company's computer network and databases, as well as to the internet from fixed and/or portable electronic devices of the Company (e.g. laptops, mobile phones, tablets), and/or data stored in them, in accordance with the Company's policy/regulation for the use of its electronic means.

9. Photographs and videos of audiovisual material concerning the employee, in the context of social events and/or promotional activities of the Company.

10. [add any other data you process if there is a legitimate purpose and legal basis for processing and the data is strictly necessary for that purpose]

The above personal data under points 1 to 7 are provided to the Company by the employee himself/herself, who must update them so that they are complete and accurate during their employment in the Company. The provision of your data is your legal obligation and a requirement for the conclusion and performance of the contract between us, which will not be possible if you refuse to provide them. Those of the above data relating to the assessment of the employee during his/her employment in the company, as well as points 8 to 9 [and 10], arise when the employee is employed in the company.

C. Purposes and legal basis for processing

The Company collects and processes the above mentioned personal data concerning the employee for the following purposes and legal bases:

1. Performance of the employment contract

The data referred to in points 1, 2, 4 and 8 above of Section B for identification, communication with the employee, professional skills and progress in the company and access to the company's systems are processed for the purpose of managing the contractual relationship under the relevant employment contract and the legal basis is the performance of the contract between the employee and the Company.

2. Keeping a register and individual employee records

The data referred to in points 3, 4, 5 and 6 above of Section B are processed for the purpose of keeping a register and individual records of employees for the fulfilment of the company's obligations arising from the legislation, i.e. labor law and/or social security and social protection law, tax law and the legal basis is the compliance of the company with a legal obligation.

3**. Execution of payroll**

The data referred to in points 1, 3 and 4 and 5 above of Section B, showing the assessment of the wage situation, the productivity bonuses, and the data under point 7 of that Section relating to the details of the employee's bank account, are processed for the purpose of carrying out the payroll and fulfilling the

company's obligation under the law and the legal basis is the compliance of the company with a legal obligation.

4. Promotion of the Company in the context of social events and/or promotional actions

The data referred to in point 9 above of Section B relating to audiovisual material shall be processed, provided that the employee has given his or her consent, which is the legal basis for processing, for the purpose of promoting the company in the context of social events and/or promotional activities.

5. Additional benefits to the employee

In order for the employee to receive the additional benefits, such as, for example, inclusion in a group insurance policy, the data referred to in points 1 and 2 of Section B shall be processed, provided that he/she has given his or her consent, which is the legal basis for processing.
In particular, for the inclusion of the employee in a group insurance policy of the company, the data referred to in points 1 and 2 of Section B may be transmitted to the insurance company cooperating with the company, provided that he/she has given his/her consent, for his/her voluntary inclusion in the collective insurance policy of the company, for which he/she then communicates with the insurance company himself/herself.

[If paragraph 5 applies, it remains, otherwise the Company shall delete it]

6) [insert any other legitimate purposes and their legal basis]

D. Transmission of data – Recipients

In order to fulfil the above mentioned functions and obligations, the Company communicates the employee's personal data to categories of persons or bodies (recipients). The recipients shall have access only to those of the employee's personal data which are strictly necessary for the performance of the tasks or the provision of the services they have undertaken towards the Company. The categories of recipients are the following:

1. Processors: the Company cooperates with processors on its behalf to assist it in fulfilling its legal or contractual obligations, which are:

- accounting service providers: company.....[110],
- providers of IT support services: company.....,
- hosting, cloud providers: company.....,
- providers of product and service promotion services: company.....,
- physical security service providers: company.....,
- [insert any other category of providers]

[110] If you wish to indicate only the categories of recipients, the information should be as specific as possible.

subject to the confidentiality of your data.

2. Financial institutions

3. Tax authorities, social security institutions, health bodies (e.g. National Public Health Organization), if provided for by law.

4. Lawyers, in so far as this is necessary for the operation of the contract, the performance of the company's statutory or contractual obligations or for the exercise of its rights and the protection of its legitimate interests

5. Bailiffs, notaries, judicial, prosecutorial and police authorities, as well as supervisory authorities, where required by legislative provisions or judicial decisions or at their legal request in the performance of their duties.

6. Co-operating insurance companies, for the inclusion of the employee in the company's group insurance policy. [if applicable, otherwise the Company shall delete it]

7. [insert any other legitimate recipients]

E. Time of data retention

Option A [specify a specific time interval]:

In the context of the employee's contract of employment with the Company, his/her data will be kept for as long as he/she retains the status of employee in the Company, and after termination for any reason of his/her employment relationship with the Company for..... [specify the legal provision on the basis of any specific legislation (indicatively, tax, insurance, labor law)].

Option B [if option A is not possible, please specify the criteria determining the time period for compliance]:

In the context of the employee's contract of employment with the Company, his/her data will be kept for as long as he/she retains the status of employee in the company, and after termination for any reason of his/her employment relationship with the Company until..... [specify the criteria determining the period of compliance, such as the expiry of the limitation period of the claims concerned[111]]

If, by the end of the above periods of time, judicial proceedings are ongoing, involving the Company and involving the employee directly or indirectly, the time for keeping the data relating to the employee shall be extended until a final judgment is delivered.

After the expiry of the above time intervals, personal data relating to the employee will be erased/destroyed [on the basis of the Company's destruction policy].

F. Transfer of data outside the EU

The Company does not transfer the employee's personal data to third countries outside the EU.

[111] The maximum period of compliance can be considered as the 20-year limitation period for civil claims between the parties under Article 937 CC.

[If the company transfers the data outside the EU then the purposes and the recipients must be indicated as follows and the above sentence shall be deleted]

The Company shall transfer to..... [insert details of the company and the country in which it is established] to fulfil its purpose..... [indicate specific purpose of transfer] with legal basis..... [indicate this legal basis] and if one of the following conditions is met at the same time [the Company should maintain the applicable condition and delete the one that does not apply]:

1) According to a decision of the European Commission, an adequate level of protection of personal data is ensured by the third country, from a territory or from one or more specified sectors in that third country;

2) In the absence of a decision as referred to in the preceding paragraph:

− the Company has provided appropriate safeguards for the transfer of personal data to third countries, in accordance with Article 46 GDPR; or

− you have given the Company your explicit consent to that effect, or

− the transfer is necessary for the performance of your employment contract, or

− the transfer is necessary for important reasons of public interest, or the establishment, exercise or defense of rights and/or legal claims of the Company; or

− the transfer is necessary for the establishment, exercise or defense of rights and/or legal claims of the Company.

[This Annex should be amended accordingly for each new transfer]

G. Employee's rights to the processing of data relating to him/her

The employee has a number of rights, in accordance with the provisions of Articles 15-22 GDPR, in relation to his or her personal data, which are processed by the Company.

The following table shows the employee's rights per processing purpose and corresponding legal basis. By selecting the corresponding right from the table below, the employee will find detailed information (concept, method and time limits for exercise) and a form for exercising it. General information on the exercise of your rights is available here.

If the employee wishes to exercise a right, he/she should fill in the corresponding form and send it to the e-mail address..... [complete the e-mail of the Company] using the employee's corporate email.

Or in writing..... [please fill in the postal address of the Company]. In this case, for the purpose of checking the identity of the applicant, a copy of the ID, passport or any other document certifying the identity of the applicant, certified by a Citizens Service Centre (KEP) or a police authority, should be attached.

PURPOSE	LEGAL BASIS	RIGHTS

Performance of the employment contract	Performance of contract (ref. 6.1.b GDPR)	Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Keeping a register and individual employee records	Compliance with legal obligation (6.1c and 9.2b for special categories)	Access (15) Rectification(16) Restriction (18)
Execution of payroll	Compliance with a legal obligation (No 6.1c)	Access (15) Rectification (16) Restriction (18)
Promotion of the company with photographs and videos depicting employees (on the website, in brochures, etc.)	Consent (No 6.1a)	Withdrawal of consent (No 7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)
Voluntary benefits to employees such as inclusion in a group insurance scheme	Consent (No 6.1a)	Withdrawal of consent (7.3) Access (15) Rectification (16) Erasure (17) Restriction (18) Portability (20)

a) the right of access, i.e. to know what data the Company keeps and processes, their origin, the purposes for which they are processed, their recipients and the time of their retention;

b) the right to erasure, i.e. to request the rectification and/or completion of his/her data, so that it is complete and accurate, providing the Company with the relevant documents to justify his/her right.

c) the right of restriction, i.e. to request the restriction of the processing of his or her data;

d) the right to data portability, i.e. to request that personal data relating to him or her which have been provided to the Company and/or transferred by the Company to another controller of his/her choice be received electronically;

e) the right to be forgotten, i.e. to request that his/her personal data be deleted from the Company's records.

Please note that the Company has the right in any event to refuse in part or in full the employee's request to restrict the processing or the erasure of his or her data, if the processing or retention of personal data relating to him or her is necessary for the performance of the employment contract, as well as for the establishment, exercise or support of its legitimate rights or the fulfilment of its legal obligations.

The Company must respond to the employee's request within one month of receipt. This period may be extended by a further two months, if necessary at the discretion of the Company, taking into account the complexity of the request and the number of requests, in which case the Company will inform the employee within one month of receipt of the extension in question and of the reasons for the delay.

If the Company does not act on the employee's request in the exercise of the above rights, or following its reply the employee considers that the above mentioned rights have been infringed, he/she may lodge a complaint with the Personal Data Protection Authority (www.dpa.gr).

H. Technical and organizational measures

The Company has taken appropriate technical and organizational measures to protect the personal data of the employee which it processes in accordance with the provisions of this Law.

List of key personal data security measures

I. Processing of data by the employee

For its part, the employee is obliged to maintain confidentiality and secrecy of any personal data of either other employees or other categories of data subjects, such as customers, suppliers, who come to their knowledge in the performance of their duties. He/she shall not communicate, transfer, store, keep or otherwise process personal data outside the tasks assigned to him/her and is not provided for in the policies and procedures of the company.

This Annex shall enter into force on the date of its signature by both parties and shall be valid for the duration of the contractual relationship between them.

The Company **The Employee**

In case the Company wishes to obtain the consent of the employee, follow the links below to the standard consent texts

a) EMPLOYEE CONSENT DECLARATION for Collection of Material from Social Events and/or Promotional Actions of the Company

B) EMPLOYEE CONSENT DECLARATION for optional employee benefits