Office of the Commissioner
for Personal Data Protection
P.O. Box. 23378, 1682 Λευκωσία
Tel.:+357 22 818 456

http://www.dataprotection.gov.cy
Email:
commissioner@dataprotection.gov.cy

GUIDE
TO COMPLETING THE RECORD OF PROCESSING ACTIVITIES

PART A- Introduction

Regulation (EU) 2016/679 for the protection of personal data comes into effect on 25 May 2018. Each public and private organisation that processes such data must comply with the Regulation. One of the main obligations stemming from the Regulation relates to keeping a Record of Activities **(Article 30).** The aim of this Guide is to provide guidance and assistance in completing the Table entitled RECORD OF PROCESSING ACTIVITIES which is attached as an Appendix and is posted on our Office's website www.dataprotection.gov.cy . This table must also be kept in electronic form **(Article 30(3)).**

Who is obliged to keep Record of Processing Activities? The obligation lies with organisations that operate as data controllers or data processors. The controller **(article 4(7))** is the person who determines the purpose and the means of processing. He can be a natural or a legal person. For enterprises, the controller is usually the owner or the managing director. However, it cannot be excluded that the data controller could be an employee, who decides on the purpose and manner of one or more processing operations. The processor **(Article 4(8))** is a person outside the organisation, to whom the controller assigns a processing operation, who acts on the instructions and on behalf of the controller. For instance, if a company decides to come into contract with a cloud service provider, this contractor shall act as data processor. In the case where there are joint controllers **(Article 26)**, the Table shall be completed by each of them, as per their particular involvement. If an organisation is based outside the European Union (EU) but offers goods or services to persons within the EU, or monitors their behaviour, then it is obliged to appoint a representative in the EU **(Articles 3(2), 27).** In such a case the representative of the organisation shall be responsible for completing the Table. If a company has an establishment in Cyprus or is a member of a group of companies **(Article 4(19))** which has its main establishment in Cyprus **(Article 4(11)**, it is recommended that the Record is completed in cooperation with other companies of the group engaged in the same or similar activities. As a rule, small and medium size enterprises with less than 250 employees are not obliged to maintain a Record of Processing Activities. **However,** if the activities of a small or medium size enterprise entail high risk for its employees or customers, then it is obliged to keep such Record. **Article 30(5)**. Keeping this Record is recommended even to organisations that are not obliged to keep it, as it is a useful tool for testing compliance with the Regulation.

What is the usefulness of keeping a Record of Processing Activities? The completion of this Record serves multiple purposes. First, an organisation is obliged to make available the Record to the Commissioner, if she asks for it. Second, it helps answering questions such as who am I, what am I doing, how do I do it and why am I doing it. It is a tool of self-understanding and self-assessing compliance with the Regulation. Third, it helps in adopting a privacy policy, if an organisation is required to have one. Fourth, it helps an organisation conform to the Principles of Accountability (**Article 5(2)**) and Transparency (**Article 5(1)(a)**). Fifth, it helps in formulating a policy or setting up mechanisms for exercise ofdata subjects' rights (**Article 12(1)).** Many organisations ask what they have to do in order to be in compliance with the Regulation and where to start from. The completion of this Record is recommended as a first step. Its proper and full

completion will help the organisation to identify certain obligations stemming from the Regulation, which must be met with. The completion of the Record of Processing Activities is not a static process. It is a continuous one, since the Record must be updated when an existing processing activity changes or a new one is added. Keeping this Record is recommended even to organisations that are not obliged to keep it, since it is a useful tool for compliance with the Regulation.

What information should be kept in the Record of Processing Activities?
A controller or his representative is obliged to keep the information referred to in columns 5-11 of the Table (**Article 30(1)**). A processor or his representative is obliged to keep the information referred to in columns 1, 4, 5, 8 and 10. However, nothing stops them from keeping additional information for reasons of self-knowledge, self-assessment, accountability and transparency. The Table attached as Appendix and posted on the Office's website, in essence, constitutes a template, which every organisation may adapt to their own particularities. An organisation may, according to its own needs, complete only the obligatory fields of the Table or additionally complete some of the non-obligatory ones or add more fields, so as to shape a spherical image of what it does, how and why it does it and for road-mapping what must be done in order to be in compliance with the Regulation.

Who must complete the Table? As stated above, the responsibility of keeping the Record lies, depending on the case, with the controller and the processor or their representatives, if any. However, they may delegate this task to one of their employees or to an external expert. If the organisation is obliged to appoint a Data Protection Officer (DPO) (**Articles 37, 38, 39**), it is recommended that the Table is completed by the DPO. In each case, the person undertaking this task must have a full picture of all the activities of the organisation. If he/she is an employee of the organisation, it is recommended that he/she is a high-ranking rather than low-ranking member, since he/she must be in continuous contact with the management and must have access to all the departments of the organisation, in order to record all the personal data processing activities. If he/she is an external associate, the organisation must provide him/her with the necessary facilitations for the proper completion of the Table. An administrative sanction (**Article 58**) or an administrative fine (**Article 83)** may be imposed on an organisation for not properly completing the Table. These are imposed on the organisation and not on the person who completed the Table. The person who will complete the Table does not necessarily have to be a lawyer or an IT. Nevertheless, he must have knowledge of the Regulation and all the legislations that the organisation applies or are applicable in the organization's field of activity, and must also have an elementary, at least, IT knowledge.

In what language must the Table be filled in? The Table must be kept in the Greek language. However, it is recommended that the Table or at least column 12, is also kept in English by organisations that carry out cross-border processing operations (**Article 4(23)**) or operate in several EU Member States, or provide information society services to children (**Article 8)** or provide information to data subjects (**Articles 13, 14**) through their website or have a mechanism available on their website for the exercise of the rights of data subjects (**Articles 15-22**). In each case, the information provided to the clients, associates or employees of an organisation must be transparent and intelligible, in easily accessible form, using clear and plain language (**Article 12(1)**).

Any practical advice? There may be a department or an individual averse to sharing information with other departments or colleagues about what it is done, how and why, or averse to sharing

adequate information easily. An employee may feel that by communicating information to his colleagues he might compromise his position. It is suggested that the person who undertakes the completion of the Table has the ability to tackle such problems. In order to complete the table, the person undertaking this task may need the assistance of organisation's IT and legal consultants. It is suggested that the person who undertakes the completion of the Table is endowed with communicative skills, so as to be able to convey technical issues to lawyers and legal issues to ITs respectively.

Below is a detailed description of the indicative information that should be filled in in each field of the Table:

PART B – Completing the Table

1. Processing Activity

In this column a brief description is given of each activity of the organisation. As a first step, it is recommended to visit each department of the organisation and take down every activity performed by each department. If the organisation has an organisational chart you would do well to study it. Some of these activities entail processing of personal data. These must be entered in this column. If an organisation has a management department, a sales department, a marketing department and a personnel department, it is advisable to divide this column into four corresponding compartments and to write their respective activities under each department. There must be a brief description for each activity. For instance, for the personnel department, two processing activities could be taken down: "Record of candidate employees" and "Record of Personnel". The description for the first could read as follows: *In this record the candidates' curriculum vitae are kept,* and the description for the second could read: *Personal files of personnel."* It is important to write down all the activities of the organisation. If the marketing department handles the organisation's website and collects visitors' browsing history through cookies, the administration of the website must be entered as a separate activity, described as *monitoring of browsing history of website's visitors.* The use of a close circuit video surveillance system must be identified as a separate activity.

2. Primary or secondary activity?

The Regulation distinguishes between main/core and auxiliary/secondary operations and imposes certain additional obligations with regard to the former as, for instance, the appointment of a Data Protection Officer (**Article 37(1)(b),(c)**). This does not mean that the personal data processed in the context of secondary operations are of less importance or that they enjoy a lower level of protection. For example, the main activity of an auditing firm would be to provide accounting services and a secondary activity would be the keeping of personnel files. Although the firm is bound by professional secrecy to protect the personal data of its clients, as well as the data of its clients' clients, when an employee takes a sick leave and brings a doctor's certificate, the health data in this certificate should enjoy a higher level of protection (**Article 9**), even though keeping such certificates constitutes a secondary processing operation. In this column next to the respective processing operation of the first column it should be listed the operations a main/core or a secondary/auxiliary one. This exercise helps to identify other obligations which an organisation is likely to be burdened with by the Regulation.

3. Legal Basis

Each processing activity must have a legal basis (**Articles 6 and 9**). In this column the article of the Regulation on which each processing activity is based, is entered. Usually, a processing operation relies only on a single legal basis. However, certain activities may have various legal bases. For example, a company keeps data relating to the employment and payroll of its employees in line with the Social Insurance Services and Taxation Department legislation (**Article 6(1)(c)**), keeps data based on the basis of the employment contract (**Article 6(1)(b)** and has a legitimate interest (**Article 6(1)(f)**) to keep information on its staff performance and advancement. Companies which operate in the investment sector or in the provision of services have a statutory obligation stemming from, the Anti-Money Laundering Law (AML), to collect information in order to assess their clients' risk. Companies which are active in the investment sector or the provision of Services, under the Anti-Money Laundering Act, are obliged to collect information in order to evaluate the risk posed by their clients. Depending on the requested service, they may collect some additional information provided for by the contracts with their clients. If for the provision of a service it is necessary to collect additional information not provided for by the Law or the contract, either from the clients themselves (**Article 13**) or from third parties (**Άρθρο 14**), subject to the Principle of data minimization (**Article 5(1)(c)**), this must be done with the consent of the clients (**Articles 4(11), 6(1)(a), 7**). Completing this field is very important since the Regulation obliges organisations to be transparent in regard to the lawfulness of each processing they perform (**Article 5(1)(a)**) and to demonstrate their compliance (**Article 5(2)**), at every stage of the processing. For some organisations, it may be easier to fill in this column after completing the column concerning the categories of data subjects.

4(a),(b). <u>Controller or Processor or their representative</u>

In column 4(a) the capacity of an organisation in relation to each processing activity is recorded, in other words, if the organisation acts as controller or processor or as the representative of the controller or the processor.

Stated in column 4(b) is the name and contact details of the person entered in column 4(a) and where applicable, the contact details of the Data Protection Officer. An organisation may offer a variety of services. For some of them it may act as controller and for others as processor. For instance, an employment bureau may operate in the field of placing candidates with employers but may also carry out interviews of its clients' applicants for work. In the first case, the said Bureau acts as data controller whilst in the second case it acts as data processor. In another case, an enterprise may operate in the field of providing consultative services for filing systems (**Article 4(6)**) kept by its clients. At the same time it may also provide to its clients storage services for digital or paper records. In the former case the company acts as controller while in the latter as processor. A supermarket assigns to a marketing company the conduct of a customer satisfaction survey. In this column must be written the name and contact details of the controller of the supermarket, as well as those of the marketing company as the processor. It is very important to state the capacity of the organisation, whether as controller or processor, for each individual processing operation, since the Regulation lays out different liabilities for the controller (**Articles 24, 25(2)**) and for the processor (**Article 28**), particularly as regards dealing with and notifying personal data breaches (**Articles 33, 34**). In certain cases, two or more organisations may act as joint controllers (**Article 26**) and decide jointly on the purpose and manner of processing. Such may be the case when, for example, a number of fast-food companies decide jointly for the creation of a call-centre for receiving and delivering orders in order to minimize their costs. When an organisation is based outside the EU but it offers goods and services to persons within the EU or monitors their behaviour, it has an obligation to appoint a representative in the EU (**Articles**

3(2), 27). If such organisation has appointed a representative in Cyprus, his capacity should be entered in column 4(a) and his name and contact details in column 4(b). The completion of this column will also help in completing column (11), since the capacity of the data controller or the processor and, where applicable, the respective responsibilities of joint controllers play an important role in carrying out an impact assessment (**Article 35**) and in the process of prior consultation (**Article 36**).

5. Purpose of processing

A brief description of the purpose of each processing operation should be given in this column. This column is directly linked to column 2, which relates to whether a processing operation is a core/primary or a secondary/ auxiliary one, to column 3 relating to the legal basis of each processing and to columns 6(b) and 9, which relate to the categories of personal data and to the scheduled time frame for their deletion, respectively. If a processing operation serves several purposes, each purpose and its description must be entered in this column. For example, a supermarket maintains as a secondary processing operation a loyalty card system, which is used only for the purpose of granting privileges or gifts to its customers. The purchases of each customer are not entered in the system. Another supermarket maintains a similar system, albeit it it is used for the purpose of granting privileges and gifts but also for sending sms messages to its customers for offers. To this end, it collects the number of its customers' mobile phones. A third supermarket has a different system which is used to provide privileges or gifts and to send promotional sms and for profiling its customers, (**Article 4(4)**) based on their consumer habits, that is, what they buy, when they buy it, their choice of products, quantities, method of payment, etc., for the purposes of planning its supply orders and for making individualized offers. All three supermarkets collect the personal data with the consent of their customers. For the first two, its activity may be deemed secondary unlike the third one which should be deemed as core/primary. In this column, each supermarket should put down the purposes it seeks to achieve through its own loyalty card system. The Regulation obliges organisations to duly inform data subjects of the purpose of each processing operation. For this reason, the completion of this column will help in completing the last column of the Table, which relates to information given to data subjects for each separate processing operation. In the example above, if the two first supermarkets decide at some stage to establish a loyalty card system similar to that of the third supermarket, they should examine if the new purposes are compatible with the initial ones (**Article 5(1)(b)**) and whether the processing of their existing customers' personal data may be based on the consent they had initially given (**Article 6(4)**). If a purpose is based on the lawful interest of the organisation (**Article 6(1)f)**), it is recommended that in this section be stated the rationale why this interest overrides the interests, fundamental rights and freedoms of the data subjects. Completion this column is of particular importance to public Authorities which offer a number of services or benefits on the basis of different legislations and must collect, in the application forms, those data which are necessary on the basis of the pertinent legislation.

6(a),(b). Categories of data subjects and categories of personal data

In column 6(a) a description of the category of data subjects to which each processing operation relates to, should be given. The data categories may correspond to customers, suppliers, associates, employees, website visitors etc., depending on the sector each organisation operates within.

As regards public Authorities, one category of data subjects could be persons who apply for a particular service or benefit. Where a category relates to children solely or it includes, it is

recommended that this be entered in column 6(a), since the Regulation includes specific provisions for children (**Articles 6(1)(f), 8, 12, 40(2)(j) and recitals 38, 58, 65, 71 και 75**). Filling in column 6(a) will help in also completing the last column of the Table which relates to information given to data subjects for each separate processing operation of an organisation. In column 6(b) shall be entered the personal data that relates to each category of data subjects. For instance, if the category of data subjects relates to a company's employees, all the categories of personal data that the company keeps on them should be listed in column 6(b)

In every case, personal data processed by an organisation should be limited to what is necessary for fulfilling the purpose of each separate processing operation (**Article 6(1)(c**). The collection of excessive information for the purposes of each processing breaches the Regulation and creates needless cost to an organisation. The exercise of column 6(b) may help in identifying useless information collected by an organisation based on past practices.

7. Categories of recipients

In column 7 shall be entered the categories of recipients (**Article 4(9)**) to whom the personal data of data subjects are likely to be communicated. For example, a travel office booking air tickets and accommodation for its customers in this column should enter as recipients, airlines and hotels. If a company has a legal obligation to communicate information concerning its customers or employees to public Authorities, it should enter in this column the general category "Public Authorities." For example, if a company which operates in the investments sector or in management services provision sector has a statutory obligation to communicate to the regulatory Authorities governing its operations, information on certain categories of its customers, it should enter in this column "regulatory Authorities" as a separate category of recipients. It must be noted that a public Authority is not considered to be a recipient when collecting information on a specific client in the frame of a particular inquiry. Although the Regulation does not require listing specific recipients but only their categories, if an organisation knows its exact recipients, it is recommended to list them in this column, as a good practice, since this may help the organisation to have a more spherical picture and to be in a position to provide better information to the persons concerned. It must be noted that in this column shall be entered also the categories of recipients to whom the data subjects themselves ask the organisation to communicate their data. Such can be, for example, the case where a company, on request by its clients, provides their banks with sale and purchase contracts for purposes of financing or loaning. In this case "clients' banks" should be listed as a distinct category of recipients. This column should also include categories of recipients in third countries to the personal data have been transferred or are intended to be transferred.

8. Transfer to third countries/international organisation

An organisation which transfers personal data to a third country, that is, outside the EU or to an international organisation (**Article 4(26)**), in this should provide information relevant to these transfers, i.e. what data are transferred, to whom they are transferred to and where the recipient is located. A data transfer may be carried out by a controller or by a processor situated in Cyprus, to a controller or processor situated in a third country or to an international organisation. The transfer may be carried out by undertakings within a group of undertakings or from one company to another or from a public Authority to another in the context of an administrative cooperation agreement. The Regulation offers a number of tools that can constitute the legal basis for making such transfers. Such tools are Adequacy Decisions (**Article 45**), Appropriate Safeguards (**Article 46**) and binding corporate rules (**Article 47**) which, as a rule, are used by groups of undertakings.

Some of these tools are subject to an approval by the Commissioner. Each organisation can choose the legal tool that serves it best, depending on its needs as well as on the purpose and type of transfer. If an organisation is in a position to prove that it cannot use any of these legal tools or that none of these tools can be used for a particular transfer, it may transfer data on the basis of derogations for specific situations (**Article 49**). However, due to the high risks associated to such transfers, this tool should be utilized only as the last resort. Transfers on the basis of derogations may require carrying out an impact assessment (**Article 35**) and/or prior consultation with the Commissioner (**Article 36**) before the intended transfer is made. The impact assessment must provide for measures to mitigate the risk entailed in this transfer. The Commissioner shall draw up and publish a list of processing operations for which carrying out an impact assessment shall be required and she may also publish a list of operations that will not require such an assessment (**Articles 35(4),(5)**). An occasional non-repetitive transfer that concerns only a limited number of data subjects can be carried out without deploying any of the aforementioned legal tools, but only for compelling legitimate purposes pursued by an organisation, which override the interests, rights and freedoms of data subjects. In such a case, the organisation must assess the risks posed by the transfer and implement appropriate safeguards. The organisation is obliged to enter in this column any information relevant to the impact assessment and to the appropriate safeguards implemented. It is recommended to additionally enter the legal tool used for each separate transfer, that is, if it is based on an adequacy decision or on appropriate safeguards or on binding corporate rules, since the organisation shall be obliged to appropriately inform data subjects (**Articles 13(1)(6), 14(1)(6)**) about each transfer. Completing this column will also help completing the last column of the Table which relates to information provided to t data subjects. Moreover, an organisation may be required to publish certain information about the lawfulness of transfers in order to demonstrate its compliance with the Regulation, in accordance with the principles of Accountability and Transparency.

9. Erasure of data

On the basis of the principle of storage limitation (**Article 5(1)(e),** when the purpose of processing is fulfilled , the data category relating to the particular processing must be erased. An organisation should list in this column the intended time limit for the erasure of data relating to each separate processing operation. Sometimes the time limit is easy to be determined, for instance when it is provided for by law; For example, for the erasure of customers' data after the end of the customer relationship and for the erasure of employees' data after the end of the employment relationship the time frames provided for by the Taxation and the Social Insurance legislation should be taken into account, respectively. Public Services take into account the particular legislation they apply and also the provisions of the State Archive Law. Organisations that operate in certain sectors, such as those of investment and finance, should study the particular legislations they apply in order to determine the time limit for erasure. Sometimes, however, it will be difficult to determine beforehand the time limit for erasing o certain categories of personal data, especially when there is a need for further processing a category of data (**Articles 5(1)(b), 6(4)**) for an organisation's legitimate interest. Where possible, the exact erasure deadline must be stated. Where this is not possible or it is difficult to specify, the estimated erasure deadline should be listed in this column. In every case, the organisation should be in a position to justify either the specific or estimated time limit. On the basis of the Regulation, in some cases before the erasure of a category of data, the organisation may be obliged to isolate certain data or restrict their processing (**Article 18**) or use encryption or pseudonymisation (**Articles 4(5), 6(4)(e), 25, 40(2)(d), 89**), particularly when the verification of the data subjects' identity is no longer necessary (**Article 11**) or when this is required by a specific Code of conduct governing the operation of an organisation (**Article 40(2)(d)**). Even

though there is no obligation to enter such deadlines in this column, it is recommended as good practice to do so, as this will help in completing column (10) relating to implemented technical and organisational security measures.

10. Technical and organisational security measures

Every organisation is obliged to implement necessary technical and organisational security measures for the safety of processing (**Article 32),** whether it operates as a controller (**Article 24(1)** or as a processor (**Article 28(1)**), especially when it is a technology firm designing and developing (**Article 25**) filing systems (**Article 4(6)**) on behalf of its clients, taking into consideration, amongst other things, the nature and purpose of the processing and the risks it entails. An organisation should describe in this column the security measures, depending on its capacity as controller or processor (**see column 4(a)**). Technical security measures could be, for example, encryption and pseudonymisation (**Articles 4(5), 6(4)(e), 25, 40(2)(d), 89**), restriction of processing (**Article 18),** back-ups, disaster recovery procedures and firewalls for the protection of online from malware software. An organisational security measure could foresee giving to members of an organisation an access role to its filing system, depending on their hierarchy (vertical access) and their duties (horizontal access), so as to ensure that each member has access only to those data required by their position and duties. Other organisational measures may include the placing a server in a secure premise with controlled access. For closed video-surveillance systems, organisational security measures impose, amongst other things, placing the monitor in a secure location and controlling, who has access to it and under what conditions. According to the Article 29 Working Party's relevant Guidelines, for notifying personal data breaches to the Commissioner (**Articles 4(12), 33)**) and for informing concerned data subjects for such breaches (**Article 34)**, the technical and organisational security measures should ensure accessibility, authenticity, integrity and confidentiality of the data (Preamble, recital 49). If an organisation operates in the provision of information technology services, the technical security measures should ensure cyber resilience. Technical measures should also be taken for the secure exercise of the right to data portability (**Article 20)**, following a request by the data subject. In the case where an organisation uses a system for profiling (**Article 4(4)**) or for automated decision making, including profiling (**Article 22),** organisational security measures must include human intervention where required. Completion this column will help in completing also the last column of the Table that relates to the elementary information which must be provided to data subjects regarding technical and organisational security measures without disclosing information that might undermine the safety of automated processing or intellectual property rights. Moreover, it may help in satisfying requests for exercising other rights, in particular the rights to access (**Article 15)** and objection (**Article 21)**.

11(a),(b). Impact assessment and prior consultation

For certain acts of processing that may involve high risk, in particular as regards the use of new technologies, it is mandatory to carry out an impact assessment (**Article 35)**, so that the organisation can apply suitable measures in order to mitigate the risk. In the case where the organisation is not certain if the intended measures will be effective in mitigating the risk or cannot think of any effective measures, it is obliged to submit the impact assessment to the Commissioner for prior consultation (**Article 36**). In column 11(a) the organisation should enter details concerning impact assessments and in column 11(b), details concerning prior consultations. The impact assessment should be carried out in four steps and therefore, in column 11(a) the following should be provided: (i) Description of the intended processing operation and of the legal basis on which it is based. (ii) How the intended processing complies with the Principles of purpose limitation and

data minimization (**Articles 5(1)(b),(c)**).(iii), the risks that this operation may entail for data subjects and (iv) the intended measures for mitigating these risks. If helpful, column 11(a) may be divided into 4 sub-columns (i), (ii), (iii), and (iv). If the organisation has appointed a Data Protection Officer (see columns 4(a), (b)), the controller should ask for his opinion on the impact assessment (**Article 35(2)**). It is therefore recommended, in column 11(a), to give a summary of the opinion of the Data Protection Officer. In column 11(b) the organisation should enter (i) the information that its obliged to provide to the Commissioner (**Article 36(3)**) in order to seek her advice and (ii) the advice it has received from the Commissioner (**Article 36(2)**). If helpful, column 11(b) can be divided in two sub-columns (i) and (ii). The completion of column 11 can help in completing column (8) which concerns the transmission of data, particularly if this is occasional and relates to a limited number of data subjects, of column (10) relating to the implementation of technical and organisational security measures, as well as of column (12), relating to information provided to data subjects.

12. Information of data subjects

Giving appropriate information to data subjects (**Articles 13, 14**) is dictated by the principles of transparency and accountability (**Articles 5(1)(a), 5(2), 12**) and constitutes the quintessence of the Regulation. The information is particularly important when a processing operation is based on the consent of the data subject (**Article 4(11)**) or when the data subject accepts the conditions included in the contract (**Article 7(4)**) or when the processing is based on the lawful interest pursued by an organisation. Depending on the category of data subjects, the information must be transparent, intelligible and in a easily accessible form, using explicit and plain language (**Article 12(1)**), particularly when given to children (**Articles 6(1)(6) και 8, Preamble references 58 and 71**). In this column the organisation should enter brief informative texts, which it intends to provide to separate categories of data subjects, for separate processing operations. If the remaining columns of the Table have been properly completed, filling in this column should be a relatively easy task. If an organisation wishes or needs to have a privacy policy, completing this column will help in editing and formulating it. Such policies may be internal, that is, be addressed to the employees of the organisation, or external, that is, addressing its customers, associates or suppliers, and users or visitors to its website. For example, if an operation relates to the use of a GPS system on an enterprise's fleet of vehicles, in this column must be stated that *"the location and movement of the vehicles may be monitored and/or recorded through the GPS system."* The respective internal privacy policy could then read: *"The use of company cars is allowed only for business purposes. The location and movement of the vehicles may be recorded and/or monitored by the administrator on behalf of the management through the GPS system."* In the case where a processing operation is based on a statutory obligation, the information text should state that the data are collected on the basis of this specific law. When an organisation communicates data to a category of recipients, the information text should state the purpose of the communication to these recipients. The information text must also include an elementary description of the technical and organisations security measures implemented by the organisation, without disclosing information that might undermine the safety of the processing or infringe on the intellectual property rights of the organisation.

PART 3 - Useful information

This Table has been designed to serve the majority of the organisations in Cyprus. It may be adapted to the needs and particularities of each organisation. If an organisation has any queries about completing any parts of the Table, it may contact our Office by telephone. However, our Office can only offer general guidance, since a thorough and in-depth knowledge is required about the identity of the organisation, what it does exactly and how. Following the enactment of the Law,

this Table may be partially modified in order to cover certain additional obligations that may arise from the said Law. In each case the attached Table covers in large part of the obligations of organisations and its completion offers a good starting point for their compliance with the Regulation.