DATA PROTECTION GUIDELINES FOR LICENSEES

Most of you have by now heard of the term data protection and the importance that is being attached to it. Data protection is being implemented in Malta through the enactment of the Data Protection Act (Chapter 440) and now as from the 25th of May 2018, through the General Data Protection Regulations.

The purpose of this Legislation is the protection of the rights of the individual in the light of advances achieved in the compilation, storage and processing of information.

The rapid advances achieved in the development of information technology means that vast amount of data can be processed and accessed in an incredibly short span of time. It is common knowledge that what only accessible up to a few years ago though a laborious process is now readily available at one's fingertips.

The general public is aware of the benefits of such developments but has also become conscious of the dangers attached to these systems being abused by their users – be it Government or others. This concern gave rise to the need for the enactment of legislation to protect against potential and actual abuse. It has to be noted that, the DPA and the GDPR will not regulate solely computer records but covers all kinds of structured data, including paper files.

What is "Personal Data"?

The term "Personal Data" refers to any information that can be attached to indentify or identifiable **natural living person**. Thus, information on companies or legal persons is not classified as personal data, which falls under the Data Protection legislation. An identifiable person on the other hand is one who can be identified by reference to one or more properties e.g his identity number, his physical, mental, economic, cultural or social identity. Data which is of a generic nature, i.e. through which no living person may be identified, is not considered as personal data. For example data collected and published in a collective manner (e.g. number of unemployed, number of unionised workers etc.) for statistical purposes and which cannot be attached to a particular person is not classified as personal data.

We have to be aware that we handle a considerable amount of information in the course of our duties. Among this information one can find that which is labelled "personal data" i.e. all covered by this person and usually consisting of name, address, telephone number etc. This is all covered by this piece of legislation, since any data (information) referring to a living person may only be handled in accordance with this Legislation. Data which besides being "personal" may additionally be classified as "sensitive" and which relates to religious and political beliefs, sex life, health, race, ethnicity or trade union membership, may only be processed under certain strictly controlled conditions and for specific purposes only.

Handling of personal Data

The question arises of how is one to be guided when handling or processing personal information. First of all is must be emphasised once more that this data must refer to a **living person –** companies and deceased persons are not covered by this Legislation.

When processing information of a personal nature one should keep the following 9 basic principles in mind:

Personal data must be:

1. *fairly and lawfully processed;*
2. *processed in accordance with good practice*
3. *collected for specific , explicitly stated and legitimate purpose;*
4. *processed strictly for the purpose it was collected;*
5. *adequate and relevant in relation to the purpose of processing;*
6. *sufficient for the purpose of processing*
7. *correct and up to date*
8. *able to be corrected, blocked or erased if found incomplete and incorrect*
9. *not kept longer than necessary*
10. *secured under lock and key in hard copy and encrypted and password protected in soft copy and saved in well secured servers.*

The above principles should provide handlers with a relatively clear set of signposts to help them along their way.

What is meant by processing in the context of this Legislation?

"Processing" and "processing of personal data" means "*any operation or set of operations taken in regard to personal data, whether or not by automatic means, and includes the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction of such data*"

The above extract helps one realise that this term covers a wide range of activities, ones which we normally take for granted in the course of our daily routine, and which we would not normally consider as "processing". Practically, processing covers every aspect of operation dealing with personal data, right from collection up to storage stage.

When one is processing personal information, one is to keep the above-mentioned 9 principles in mind. Remember that today's data processor (i.e. the person handling the data) might be tomorrow's "data subject" (i.e. a natural person to whom the data relates). In simple terms, your own personal data will sooner or later (and certainly more sooner than later) be in the possession of others and you would surely not feel comfortable having it processed in a careless manner!

It might be appropriate to go through the above principles in greater detail in order to be in a better position to fully understand what they imply.

• Fair, lawful processing in accordance with good practice

It is of utmost importance that the data subject is primarily informed of the purpose for which his/her information is to be used. Normally this is done at the point of collection, particularly on the forms used. The basic idea behind these limitations is that the data that is being processed is used

solely for the purpose it was collected for and in accordance with legislation. For example, if the data were collected for the processing of an application for the issue of a licence their use should be strictly limited to this end and for no other purpose, unless the data subject gives his/her consent in writing, or except where provided otherwise by any other specific Act.

Processing should be carried out strictly in accordance with the provisions of this Legislation – i.e. information should never be revealed to third parties (unless the data subject has given his/her written authority).

All personal data must be secured and protected against manipulation, loss or access by unauthorised parties.

• Collected for specific, explicitly stated and legitimate purposes

This condition is intimately attached to the previous one. The purpose for which the information is collected must be clearly stated and in accordance with the need to satisfy a legal obligation.

• Processed strictly for the purpose it was collect

This condition is pretty self-explanatory. The data that are collected in the course of our duty must be used exclusively to carry out that particular process and for none other.

• Adequate, relevant, not excessive and accurate

The data that are collected and processed for a particular task should be the minimum required to execute that particular job. If a client is applying for a passport, there is no need to ask him to provide information on how often he goes abroad, the purpose for the visits abroad, the make and colour of his car etc. We must never fall into the trap of requesting more information than that which is strictly required in the belief that one day we might require it. Care must be taken at all times to ensure accuracy of data and immediate steps should be taken to correct or delete any errors that might crop up.

• Data should be able to be corrected if incomplete

Systems and procedures should be designed in such a way that it makes it possible that wherever data is incomplete, it can be rectified, completed, blocked or erased, taking into consideration the purpose for which it was collected. An example of when this can happen is where the Commissioner for Data Protection issues such in cases of non-conformity to the law.

• Data should not be kept longer than necessary

We have a tradition of keeping information indefinitely and certainly beyond its “use by date”. Once the data have been processed and the service given, there should not be any need to retain the information beyond a reasonable period. A policy will need to be devised whereby “expired” data are disposed of in an organised manner. One also has to keep in mind the provisions of the Archives Act.

Note:

The above information has been compiled and bought to your attention to help you become aware of current Data Protection Legislation and the responsibility that we all share in protecting each and every individual's privacy.

It should also provide you, the user, with a brief overview and guidelines on data protection.

The generic email address of the Data Protection Officer of the Health Care Standards Directorate is gdpr.hcs@gov.mt. Should you have any queries regarding data protection issues kindly use this email address.

Dr Elizabeth Xuereb

Data Protection Officer

Health Care Standards Directorate

Issued on: 31/05/18