DATA PROTECTION LAWS OF THE WORLD

Malta

DLA PIPER

MALTA

Last modified 26 January 2017

LAW

The relevant law is the Data Protection Act (Act) (Chapter 440 of the Laws of Malta) and the Regulations (at present nine in number) issued under it.

DEFINITIONS

Definition of personal data

Personal data is defined in the Act as:

'...any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

Definition of sensitive personal data

Sensitive personal data is also defined in the same Act as meaning:

'...personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life'.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Information and Data Protection Commissioner Airways House

Second Floor
High Street
Sliema SLM 1549
Malta

T +356 2328 7100
F +356 23287198

idpc.info@gov.mt

www.idpc.gov.mt

The Information and Data Protection Commissioner ('Commissioner') has the function (among others) of generally ensuring the correct processing of personal data in order to protect individuals from violations of their privacy.

REGISTRATION

Controllers of data (defined in the Act as persons who alone or jointly with others determine the purposes and means of the processing of personal data), unless exempted by the Commissioner in the circumstances mentioned in the Act or in the circumstances mentioned in Subsidiary Legislation 440.02, must generally notify the Commissioner before carrying out wholly or partially automated processing operations or a set of such operations which are intended to serve either a single or several related purposes. The Commissioner maintains a Register of processing operations which have been notified to him.

The Register must contain the following information:

- the name and address of the data controller and of any other person authorised by him in that respect, if any
- the purpose or purposes of the processing
- a description of the category or categories of data subject and of the data or categories of data relating to them
- the recipients or categories of recipient to whom the data might be disclosed, and
- proposed transfers of data to third countries.

DATA PROTECTION OFFICERS

Under Maltese law there is presently no obligation to appoint data protection officers. However, the Act states that the controller of personal data shall notify the Commissioner on the appointment or removal of a personal data representative (if any). The personal data representative has the function (among others) of independently ensuring that the controller processes personal data in a lawful and correct manner and in accordance with good practice and in the event of the personal data representative identifying any inadequacies, he shall bring these to the attention of the controller.

COLLECTION & PROCESSING

Personal data may be processed (which includes also the collection of data) only if:

- the data subject has unambiguously given his consent
- processing is necessary for the performance of a contract to which the data subject is a party to or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed, or
- processing is necessary for a purpose that concerns a legitimate interest of the controller, or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

If the data subject gives notice to the controller of his opposition, personal data cannot be processed for the purposes of direct marketing.

As a general rule, sensitive personal data cannot be processed except in the cases mentioned in the Act (e.g. where the data subject has given his explicit consent to processing or has made the data public).

The data subject has a right to be provided, by the controller or any person authorised by him, with information such as the identity and habitual residence, or principal place of business, of the controller and of any other person authorised by him in that respect; the purpose of the processing; and any further information relating to matters such as the recipients of the data, whether the reply to any questions made to the data subject is obligatory or voluntary and the existence of the right to access, rectify and erase the data concerning him. The controller must guarantee fair processing in respect of the data subject.

TRANSFER

The controller must always notify the Commissioner of any proposed transfers of data to third countries, since such transfers also constitute 'processing' under Maltese law. 'Third countries' only include countries which are not Member States of the European Union. The transfer may only take place if the third country to which the data is to be transferred ensures an adequate level of protection. Whether the country ensures such a level of protection shall be decided by the Commissioner.

A transfer of data to a third country that does not ensure an adequate level of protection may still be effected by the controller but only if the data subject gives his unambiguous consent to the proposed transfer or if the transfer:

- is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request
- is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party
- is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims
- is necessary in order to protect the vital interests of the data subject, or
- is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

In the instances listed above, the Commissioner's approval is not generally required but the transfer must still be notified and in some cases, the Commissioner may still object to the transfer if certain adequate safeguards are not in place. In fact, the Commissioner has the power to *authorise* such a transfer of personal data to a third country that does not ensure an adequate level of protection provided however that the controller provides the said adequate safeguards, such as by contractual provisions (including the EU Model Clauses), with respect to the protection of privacy and fundamental human rights.

The way this seems to be interpreted by the Maltese Office of the Information and Data Protection Commissioner (IDPC) is that despite the grounds listed above (including consent of the data subject), the Commissioner may still require the said adequate safeguards before authorising a transfer to a third country not offering an adequate level of protection. The EU Model Clauses and/or Binding Corporate Rules (for intra-group transfers) are often invoked by controllers wishing to transfer personal data to such countries. In these cases the Commissioner's approval is not automatic and applicants must file evidence of any additional safeguards that may exist.

The Minister responsible for freedom of information and data protection may also designate by Order, in order to implement any international convention to which Malta is party or any other international obligation of Malta, that the transfer of personal data to any country listed in the Order shall not be restricted on grounds of protection of privacy.

For the avoidance of all doubt, it should be noted that apart from mere notification to the Commissioner, no other restrictions or formalities apply in relation to transfers of personal data to:

- Member States of the European Union
- Member States of the European Economic Area (EEA)
- Third countries which are recognised by the EU Commission to have an adequate level of protection.

Transfers of personal data based on the EU standard contractual clauses may require prior authorisation from the IDPC depending on the 'third country' in question. As stated above, if the said third country is an EU/EEA country and/or an EU Commission-white-listed country then, apart from the notification obligation, no prior *authorisation* from the IDPC is required.

It should be noted that following the judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbour regime is no longer regarded as a valid basis for transferring personal data to the United States of America (USA). Data Controllers previously relying on the 'safe harbour' scheme to transfer personal data from Malta to the USA, are therefore required to use alternative mechanisms as provided for under national law in order to guarantee an adequate level of data protection for such transfers. *Prior Approval* by the Commissioner for such transfers is now required – as opposed to mere *notification* – in those cases previously relying exclusively on the 'safe harbour' procedure.

On 2 February 2016, the European Commission unveiled the so-called "EU-U.S. Privacy Shield Framework" (the Framework) - an agreement reached between the European Union and the United States of America on international data transfers.

On 12 July 2016, the European Commission adopted its decision on the Framework, deeming it adequate to enable data transfers under EU law. Therefore, going forward, although the safe harbour mechanism (which required only mere notification) no longer exists, authorisations from the Maltese IDPC may be provided on the basis of this Framework. In the immediate future, the IDPC will likely authorise transfers of data from Malta to those U.S.-based organisations that are self-certified in terms of the EU-U.S. Privacy Shield Framework (see https://www.privacyshield.gov/welcome) and that publicly commit to comply with the Framework's requirements.

However, in all other cases where personal data will be transferred from Malta to the USA and where the Framework does *not* apply, the IDPC will require safeguards such as Standard Contractual Clauses contained in data transfer agreements (based on the EU Model Clauses) and/or Binding Corporate Rules (BCRs). Authorisations/Prior Approvals are granted very much on a case-by-case basis depending on the circumstances of the case at hand.

SECURITY

Data controllers must implement the appropriate technical and organisational measures to protect personal data which is processed against accidental destruction or loss or unlawful forms of processing. An adequate level of security must be provided which gives regard to:

- the technical possibilities available
- the cost of implementing the security measures
- any special risks that exist in the processing of personal data, and
- the sensitivity of the personal data being processed.

If a processor is engaged by the controller, the controller must ensure that the processor can implement the necessary security measures and that the processor actually takes such measures.

BREACH NOTIFICATION

Legal Notice 239 of 2011, which was brought into force as of 1st January 2013, has amended Subsidiary Legislation 440.01, Processing of Personal Data (Electronic Communications Sector) Regulations, making new provisions for breach notifications.

The Regulations provide that, in the case of a personal data breach, **providers of publicly available electronic communications services** must notify the breach to the Commissioner without delay. 'Personal data breach' is defined in the Regulations as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service'*.

If the breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must also notify the subscriber or individual of the breach without delay. However, notification to the subscriber or individual concerned shall not be required on the condition that the provider demonstrates to the satisfaction of the Commissioner that he has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security

breach. Such technological protection measures should render the data unintelligible to any person who is not authorised to access it.

If the provider has not already notified the subscriber or individual of the personal data breach, the Commissioner may require the provider to do so after considering the likely adverse effects of the breach.

The notification to the subscriber or individual must at least include the nature of the breach and the contact points where more information can be obtained. The notification must also recommend measures to mitigate the possible adverse effects of the breach. The notification to the Commissioner shall also include the consequences of and the measures proposed or taken by the provider to address the breach. The Regulations also provide that the Commissioner is to encourage the drawing up of guidelines and where necessary issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format that such notification is to take and the manner in which the notification is to be made.

Service providers are to maintain an inventory of personal data breaches consisting of the facts surrounding the breach, its effects and the remedial action taken which must be sufficient to enable the Commissioner to verify compliance with the provisions of the Regulations.

ENFORCEMENT

The Act states that any person who does not comply with any lawful request relevant to an investigation by the Commissioner shall be guilty of an offence under the Act.

In the exercise of his functions under the Act, the Commissioner has the same powers to enter and search any premises as are vested in the executive police by any law as may be in force from time to time.

If the Information and Data Protection Commissioner concludes that personal data is processed or may be processed in an unlawful manner, the Commissioner shall order rectification, and if rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data to continue processing the personal data in any manner other than to store that data.

If the controller does not implement security measures in terms of the Act, or transfers personal data to third countries in contravention of the Act or fails to notify the Data Protection Commissioner in terms of the Act, the Commissioner may impose an administrative fine as prescribed (see below for more information on fines and penalties).

Where the Data Protection Commissioner decides that personal data has been unlawfully processed, the said Commissioner shall by notice order the controller of personal data to erase the personal data.

Any person aggrieved by a decision of the Commissioner shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within thirty days from the notification to him of the said decision.

Any party to an appeal to the said Tribunal who feels aggrieved by a decision of the Tribunal, or the Commissioner if he feels aggrieved with any such decision, may on a question of law appeal to the Court of Appeal of Malta within thirty days from the date on which that decision has been notified.

It should be noted that if controllers feel aggrieved by a decision of the Commissioner to order the erasure of personal data, the controller of personal data must (within fifteen days from the receipt of the Commissioner's notice) seek redress, by requesting (by way of application) the Court of Appeal of Malta to revoke the order of the Commissioner.

Fines and Penalties

Recently, the Act has been amended to address two separate frameworks, one for administrative fines that may be imposed by the Commissioner and another for court penalties. A clear distinction between administrative fines and court penalties was introduced by means of a separate definition for each of the two types of sanctions and the Act now establishes a procedure for their imposition. Moreover, schedules to the Act were introduced in order to assist, inter alia, in identifying which of the offences are liable to administrative fines and which are liable to court penalties. Parameters were also established with regards to the minimum and maximum amount of fines and penalties that may be imposed for each respective breach.

Sanctions under the Act are both civil and criminal. A data controller in breach of the Act may, inter alia, be liable (for each violation/offence) to: (i) an administrative fine imposed by the Commissioner; (ii) an order to pay compensation to the aggrieved data subject following a successful action for damages by the data subject; or (iii) a criminal fine (currently a maximum of EUR23,300) or imprisonment (currently a maximum of six months) or both.

1. The various administrative fines that may be imposed by the Commissioner vary in nature (there are three levels of fines) and must be examined on a case-by-case basis. The maximum fine that may be imposed is of EUR 23,300 for each violation with an additional (maximum) of EUR 2,500 as a daily fine for each day during which the violation in question subsists. Fines of this nature are generally deemed as civil debts in favour of the Commissioner.

2. An aggrieved data subject may, by sworn application filed in the competent Civil Court, exercise an action for damages against a data controller who processes data in contravention of the Act. Such action must be commenced within 12 months from the date when the said data subject becomes aware or could have become aware of such a contravention, whichever is the earlier.

3. The various (criminal) penalties which are enforceable by prosecution in the Courts of Malta also vary depending on the offence in question (here too, there are three levels of penalties). The maximum penalty ('multa') that may be imposed is of EUR 23,300 per violation or a term of imprisonment of not more than six months (per violation) or both such fine and imprisonment (depending on the matter at hand).

ELECTRONIC MARKETING

The Act applies also to most electronic marketing activities since in the course of such activities, it is likely that 'personal data' as defined above (including e-mails) will be 'processed' as understood by the Act. In relation to direct marketing (even electronic), consent may be revoked at will by the data subject(s). The controller is legally bound to inform the data subject that he/she may oppose such processing at no cost.

Apart from the Act, the 'Processing of Personal Data (Electronic Communications Sector) Regulations 2003' (Legal Notice 16 of 2003 as amended) (the 'Electronic Communications Regulations') address a number of activities relating specifically to electronic marketing.

In the case of subscriber directories, the producer of such directories shall ensure (without charge to the subscriber) that before any personal data relating to the subscriber (who must be a natural person) is inserted in the directory, the subscriber is informed about the purposes of such a directory of subscribers and its intended uses (including information regarding search functions embedded in the electronic version of the directories). No personal data shall be included without the consent of the subscriber. In furnishing his consent the subscriber shall determine which data is to be included in the directory and he is free to change, alter or withdraw such data at a later date. The personal data which shall be used in the directory must be limited to what is necessary to identify that subscriber and the number allocated to him, unless the subscriber has given his additional consent authorising the inclusion of additional personal data.

The Electronic Communications Regulations also deal with the issue of unsolicited communications. A person is prohibited from using any publicly available electronic communications service to engage in unsolicited communications for the purpose of direct marketing by means of:

- an automatic calling machine
- a facsimile machine, or
- electronic mail

to a subscriber, irrespective of whether such subscriber is a natural person or a legal person, unless the subscriber has given his prior explicit consent in writing to the receipt of such a communication.

By way of exception to the above, where a person has obtained from his customers their contact details for electronic mail in

relation to the sale of a product or a service, in accordance with the Act that same person may use such details for direct marketing of its own similar products or services. However, the customers must be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

Allowing the recipient to send a request requesting that such communication cease, is strictly prohibited.

In all cases the practice of inter alia sending electronic mail for the purposes of direct marketing, disguising or concealing the identity of the sender or without providing a valid address to which the recipient may send a request that such communications cease shall be prohibited.

ONLINE PRIVACY

Cookie Compliance

Legal Notice 239 of 2011 entitled 'Processing of Personal Data (Electronic Communications Sector)(Amendment) Regulations 2011' was brought into force with effect as of 1st January 2013. This Legal Notice amended the regulations thereby implementing into Maltese Law the amendments under Article 2(5) of Directive 2009/136/EC. Having said the above, the IDPC is yet to issue local guidelines on the way in which the so called 'cookie clause' is to be interpreted. We have no information indicating when these guidelines may be published. It is worth noting that the IDPC's website presently makes reference to the Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies (adopted on 2 October 2013).

Traffic Data

Under the Electronic Communications Regulations, traffic data relating to subscribers and users processed by an undertaking which provides publicly available electronic communications services or which provides a public communications network, shall be erased or made anonymous when it is no longer required for the purpose of transmitting a communication.

Traffic data required for the purposes of subscriber billing or interconnection payments may be retained provided however that the retaining of such data shall only be permissible up to the period during which the bill may be lawfully challenged or payment pursued.

Furthermore, traffic data may be processed where the aim is to market or publicise the provision of a value-added service, however, the processing of such data shall only be permissible to the extent and for the duration necessary to render such services.

Processing of traffic data is also permissible by an undertaking providing publicly available electronic communication for the following purposes:

- managing billing or traffic management
- customer enquiries
- fraud detection, and
- rendering of value-added services.

Location Data

Where location data (other than traffic data) relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision a value-added service.

Prior to obtaining the user or subscriber's consent, the undertaking providing the service shall inform them of the following:

- the type of location data which shall be processed

- the purpose and duration of processing, and
- whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service.

A user and/or subscriber may withdraw their consent for the processing of such location data (other than traffic data) at any time.

KEY CONTACTS

Mamo TCV Advocates
www.mamotcv.com/

Dr. Antoine Camilleri
Partner
T +356 21 231 345
antoine.camilleri@mamotcv.com

Dr. Claude Micallef-Grimaud
Senior Associate
T +356 21 231 345
claude.micallefgrimaud@mamotcv.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.