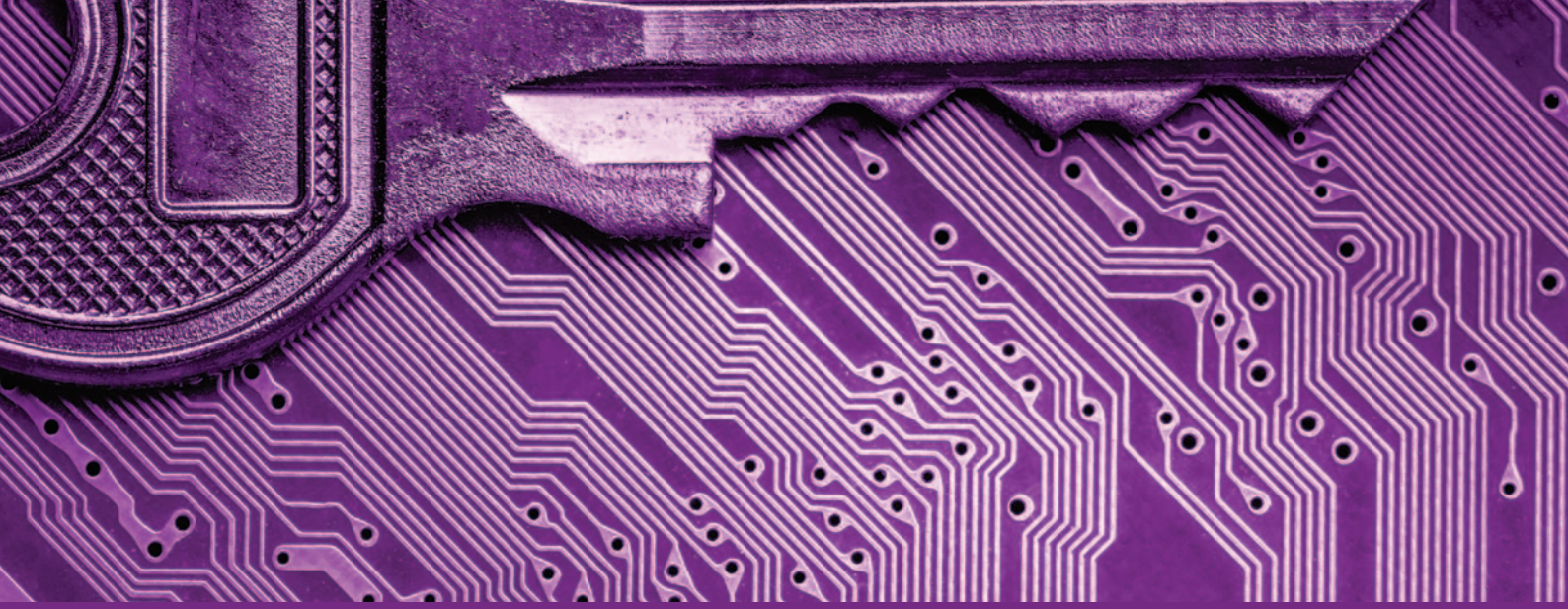

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

glg
global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf →

global legal group

Country Question and Answer Chapters:

Malta

Dr. Paul Micallef Grimaud

GANADO Advocates

Dr. Luke Hili

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

As of 25 May 2018, the principal data protection legislation in the EU is Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and led to increased (though not total) harmonisation of data protection law across the EU Member States.

The provisions of the GDPR are complemented by Maltese legislation, namely the Data Protection Act ("**DPA**"), Chapter 586 of the Laws of Malta and various pieces of subsidiary legislation implemented under the same Chapter 586.

1.2 Is there any other general legislation that impacts data protection?

General legislation which currently impacts data protection includes:

- Processing of Personal Data (Protection of Minors) Regulations (Subsidiary Legislation 586.04).
- Transfer of Personal Data to Third Countries Order (S.L. 586.05).
- Restriction of Data Protection (Obligations and Rights) Regulations (S.L. 586.09).

1.3 Is there any sector-specific legislation that impacts data protection?

Current sector-specific legislation relating to data protection includes:

- Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01).
- Processing of Personal Data for the purposes of the General Elections Act and the Local Councils Act Regulations (Subsidiary Legislation 586.06).
- Processing of Personal Data (Education Sector) Regulations (Subsidiary Legislation 586.07).
- Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations (Subsidiary Legislation 586.08).
- Processing of Data concerning Health for Insurance Purposes Regulations (Subsidiary Legislation 586.10).
- Processing of Child's Personal Data in relation to the Offer of Information Society Services Regulations (Subsidiary Legislation 586.11).

1.4 What authority(ies) are responsible for data protection?

The relevant data protection regulatory authority is the Information and Data Protection Commissioner ("**IDPC**").

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" or "Special Categories of Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- "**Data Breach**" means 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.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  This is not applicable.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

As expected, Maltese law does not broaden or narrow the territorial scope of the GDPR. In addition, the Data Protection Act and subsidiary legislation enacted under it apply to:

(i) the processing of personal data by a controller or processor established in Malta, regardless of where the processing takes place;

(ii) the processing of personal data of data subjects who are in Malta by a controller or processor not established in the European Union, where the processing activities are related to:

  (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Malta; or

  (b) the monitoring of their behaviour in so far as their behaviour takes place within Malta; and

(iii) the processing of personal data by a controller not established in the European Union but in a place where the laws of Malta apply by virtue of public international law.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. Article 6(1) of the GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Businesses require stronger grounds to process sensitive personal data (special categories of data). The processing of sensitive personal data is, in accordance with Article 9(2) of the GDPR, only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; (iii) the processing is in the vital interest of the data subject or third parties where the data subject is incapable of providing consent; (iv) the data has been publicly revealed by the data subject; or (v) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**

  The right to protection of personal data is not an absolute right and must be considered in relation to its function in society and be balanced against other fundamental rights in a proportional manner.

- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- *Other key principles – please specify*

  Data Security – Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

  Accountability – The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes for which the data is being processed; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data was not

collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data is erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**

  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data is no longer needed for the original purpose (and no new lawful purpose exists); (ii) in the event that the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data has been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law. This right is, however, limited in the cases expressly mentioned in Article 17(3) of the GDPR which are related, in the main, to public interest, the freedom of expression and information, legal obligations imposed on the controller to process the data, the exercising of official authority vested in the controller and the establishment, exercise or defence of legal claims.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or the processing is necessary for the purposes of the legitimate interests pursued by the controller. In such a case, the controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or where the processing is required for the establishment, exercise or defence of legal claims.

- **Right to restrict processing**

  Data subjects have the right to restrict the processing of personal data, which means that, with the exception of storage, the data may only be processed by the controller with the data subject's consent, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or a Member State if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for the original purpose, but the data is still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**

  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**

  A data subject has the right to withdraw his consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints concerning the processing of their personal data with the IDPC, if the data subjects live in Malta or the alleged infringement occurred in Malta.

- *Other key rights – please specify*

  Not applicable.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The GDPR does away with the general obligation of notifying the supervisory authority (the IDPC) prior to processing personal data. However, Article 7 of the DPA necessitates consultation and prior authorisation with the IDPC where the data controller intends to process, in the public interest:

- genetic data, biometric data or data concerning health for statistical or research purposes; or
- special categories of data in relation to the management of social care services and systems, including for purposes of quality control, management information and the general national supervision and monitoring of such services and systems.

Moreover, in accordance with Article 36 of the GDPR, the IDPC should be consulted where, notwithstanding reasonable mitigating measures taken in terms of available technologies to address high risks following the carrying out of a Data Protection Impact Assessment ("**DPIA**"), residual risks would still be present.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable – please see question 6.1.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable – please see question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable – please see question 6.1.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable – please see question 6.1.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable – please see question 6.1.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable – please see question 6.1.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable – please see question 6.1.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable – please see question 6.1.

6.10 Can the registration/notification be completed online?

This is not applicable – please see question 6.1.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable – please see question 6.1.

6.12 How long does a typical registration/notification process take?

This is not applicable – please see question 6.1.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

As per Article 37 of the GDPR, designation of a DPO shall be mandatory where:

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

(b) the core activities of the data controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or

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

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in a wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The appointment of a single DPO covering a group of undertakings is permissible provided that the DPO is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Notification to the IDPC will need to be carried out in relation to the appointment of a DPO.

Notification of appointment of a DPO to the IDPC normally entails the provision of the following details:

- Data Controller.
- Name of DPO.
- Position.
- Mailing Address.

- Email Address.
- Contact Number.
- Nature of Business.
- Date of Appointment and whether the DPO is fulfilling this role for other data controllers.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The details of the Data Protection Officer must be published although not necessarily named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**"), today the European Data Protection Board ("**EDPB**") recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the obligations imposed on the controller in relation to the appointment of processors when, in turn, appointing sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Data subject consent provided for the purpose of electronic marketing in accordance with Article 6 of the GDPR requires a clear, affirmative act which is given through an active motion or declaration. Moreover, guidance issued by the Article 29 Working Party reiterates that a data subject's consent cannot be obtained by way of a blanket acceptance of general terms and conditions of a service, for instance. Consequently, prior opt-in consent is required.

This said, where the nature of the goods/services being marketed are such that the data controller may be said to have a *legitimate interest* in processing a data subject's personal data, consent will no longer need to be obtained in order to lawfully process said data (for example: where the goods/services marketed are *directly* linked to the existing relationship between the data controller and the data subject).

Moreover, the controller must inform the data subject of his right to object at no cost, to the processing of his personal data for direct marketing purposes.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

With respect to other means of marketing including unsolicited communications by automated calling machines or fax, the subscriber (both a natural or legal person) must give their prior consent to their personal data being used for direct marketing purposes. In terms of direct marketing carried out by post, consent under the GDPR is understood not to be required, provided that the data controller may prove a legitimate interest in marketing his goods/services.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, such restrictions apply to marketing sent from other jurisdictions.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, the IDPC has dealt with cases involving breaches of marketing restrictions both prior to, and after, the entry into force of the GDPR.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful; however, the entity making such marketing list available should inform the data subjects and obtain their clear and unequivocal consent to the sale of their data by the controller to third parties, prior to such sale taking place. Where the marketing list has been purchased, the information requirements listed in Article 14 of the GDPR would apply.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Maltese law does not cater for penalties, other than those which may be imposed under the GDPR, in the case of marketing communications that are sent in breach of applicable restrictions.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Currently, Malta implements Article 5 of the ePrivacy Directive (which was transposed into Maltese law by way of the Processing of Personal Data (Electronic Communications Sector) Regulations, S.L. 586.01). Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Currently, there is no distinction as regards different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To our knowledge, the IDPC has not taken any enforcement action in relation to cookies as yet.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Maltese law does not cater for penalties, other than those which may be imposed under the GDPR, in the case of breaches of cookie restrictions.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

Moreover, Article 10 of the DPA stipulates that in the absence of an Adequacy Decision delivered by the EU Commission, the Minister responsible for data protection may, following consultation with the IDPC, by regulations set limits to the transfer of specific categories of personal data to a third country or an international organisation for important reasons of public interest.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. Some common options include the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as data exporter) and a processor (as data importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In those instances referred to in questions 11.1 and 11.2 above (i.e., (1) where the data importer is established in a EEA Member State, (2) where the data importer is established in a state benefitting from an Adequacy Decision, or (3) where the abovementioned appropriate safeguards are in place to validate the data transfer), notification to the IDPC is not required.

Notification to the IDPC is, however, required in any such case where the data transfer not only lacks the measures mentioned above, but also fails to adhere to those conditions set out in Article 49 of the GDPR which allow for derogations in specific situations.

Moreover, as regards Standard Contractual Clauses, authorisation from the IDPC is not required. Conversely, in the case of BCRs,

these must be approved by the IDPC. Alternatively, where appropriate safeguards are adopted in the form of *ad hoc* contractual clauses or, in the case of public bodies, by means of provisions inserted in administrative arrangements, these must first be authorised by the IDPC.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Protection of the Whistleblower Act, (herein the "**PWA**") (Chapter 527 of the Laws of Malta) provides protection to employees in both the private sector and public administration to disclose information regarding improper practices.

The term "employee" is defined as:

(a) a person who has entered into or works under a contract of service with an employer, and includes a contractor or subcontractor who performs work or supplies a service or undertakes to perform any work or to supply services;

(b) any person who has undertaken personally to execute any work or service for, and under the immediate direction and control of, another person, including an outworker, but excluding work or service performed in a professional capacity to which an obligation of professional secrecy applies when such work or service is not regulated by a specific contract of service;

(c) any person in employment in the public administration;

(d) any former employee;

(e) any person who is or was seconded to an employer;

(f) any volunteer in terms of law; and

(g) any candidate for employment, but only where information concerning a serious threat to the public interest constituting an improper practice has been acquired during the recruitment process or at another pre-contractual negotiating stage.

The scope of a report made in terms of the PWA is "improper practice". This term includes an action or series of actions whereby:

(a) a person has failed, is failing or is likely to fail to comply with any law and/or legal obligation to which he is subject;

(b) the health or safety of any individual has been, is being or is likely to be endangered;

(c) the environment has been, is being or is likely to be damaged;

(d) a corrupt practice has occurred or is likely to occur or to have occurred;

(e) a criminal offence has been committed, is being committed or is likely to be committed;

(f) a miscarriage of justice has occurred, is occurring or is likely to occur;

(g) bribery has occurred, is occurring or is likely to occur;

(h) a person acts above his authority; or

(i) information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

The provisions of the PWA do not apply to members of a disciplined force, members of the Secret Service or persons employed in the foreign, consular or diplomatic service of the Government.

One should also take note of the EDPB (formerly, Article 29 Working Party) Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes. This is limited to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The EDPB recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

No, it is not prohibited. However, anonymous reporting is not protected in terms of the PWA. Such an anonymous report may still be taken into account to determine whether an improper practice has occurred. If upon consideration of all circumstances, the report is deemed to be defamatory or libellous, it shall be discarded.

Additionally, anonymous reporting is not prohibited under the GDPR; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the EDPB considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process and, in particular, will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No registration and/or notification to the IDPC is required in this respect. A high-visibility sign would suffice as an adequate form of notice. However, it must be kept in mind that a data protection impact assessment ("**DPIA**") should be undertaken with assistance from the DPO when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the IDPC.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy

of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the data processing would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

The use of surveillance cameras must have a clearly defined specific purpose which is proportionate to the rights to privacy of individuals. The IDPC has also issued guidelines as to the use of biometric equipment at the workplace, establishing that this is only permissible in places demanding a high level of security and strict identification procedures.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The processing of employee data under GDPR is permitted in so far as it is necessary for the purposes of the employment of the data subject and the processing carried out is proportionate to this need. The processing of employee personal data must be carried out on one of the legal bases listed in Article 6(1) or, in case of sensitive data, Article 9(2) of the GDPR. The Maltese Court of Appeal has recently confirmed that an email address consisting of the name and surname of the employee combined with the IP address of the company with which she was employed, constituted personal data and the employer could not have processed the said personal data by accessing the email account of the employee without giving appropriate notice which, in the circumstances, would have been proportionate to the employer's needs to access the said personal data.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As mentioned above, processing of an employee's personal data must be carried out on one of the legal bases provided for in the GDPR. Where the employer needs to rely on "consent" – such as in the case of uploading photos on the employer's website where there is no other ground, such as legitimate interest, for processing the data – the employer must ensure that the employee is informed that the consent should be freely given and that there would be no adverse consequences if he/she were to opt not to provide such consent. Moreover, employees should be informed of the processing activities relating to their data, generally through a privacy policy.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As regards biometric scanning, the IDPC had established in its past guidance that, where employees are unionised, it is preferable for the employer to consult with the respective union. This is not an obligation under the GDPR and the DPA.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; the ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The data controller shall be responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the IDPC, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach, and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover, depending on the nature of the breach.

The DPA also makes specific reference to administrative fines on public authorities or bodies, stating that any such fine shall not exceed, in the aggregate: €25,000 for each violation, along with daily fines of €25 for every day during which the violation persists, in relation to violations under Article 83(4) of the GDPR; and €50,000 for each violation, along with daily fines of €50 for every day during which the violation persists, in relation to violations under Article 83(5) or (6) of the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.	Not applicable.
Corrective Powers	The IDPC has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).	Not applicable.
Authorisation and Advisory Powers	The IDPC has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.	Not applicable.
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year. *Ad hoc* fines for public authorities apply (see details in 15.4, above).	Not applicable.
Non-compliance with a data protection authority	Not applicable.	The DPA states that without prejudice to the provisions of Articles 21 and 83 of the GDPR, any person who (1) knowingly provides false information to the IDPC when so requested by it pursuant to its investigative powers, or (2) does not comply with any lawful request pursuant to an investigation by the IDPC, shall be guilty of an offence and, on conviction, be liable to a fine (*multa*) of not less than €1,250 and not more than €50,000 or to imprisonment for six months, or to both such fine (*multa*) and imprisonment.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing. A court order is not required.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The IDPC tends to scale its approach to enforcement measures depending on the gravity of the breach and the manner in which the controller/processor in question rectifies and responds to the breach. This said, there are no official guidelines or annual reports (post 2011) published by the IDPC.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

To our knowledge, the IDPC has, to date, not exercised its powers against businesses established in other jurisdictions although, under the GDPR, it is entitled to do so in those instances in which it would be deemed to be the competent authority.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Maltese businesses will typically respond to requests for disclosure emanating from public authorities having the power under Maltese law to make such requests. Requests for the provision of information, including personal data, in the context of police investigations could only be made by the executive police under the ordinary Maltese criminal procedures.

17.2 What guidance has/have the data protection authority(ies) issued?

The IDPC has not issued any guidance on this point.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

No formal reports are available from the IDPC. We are, however, aware of the fact that the IDPC has been rather active in ensuring compliance with the obligations of the GDPR through various reports being submitted to it, including a number of data breach notifications. In accordance with a February 2019 GDPR Data Breach Survey issued by DLA Piper, it transpires that, until such date, the IDPC had issued approximately 17 fines. This is a significant change to the approach towards enforcement and awareness of data protection obligations in Malta.

18.2 What "hot topics" are currently a focus for the data protection regulator?

No particular trends have emerged.

Dr. Paul Micallef Grimaud
GANADO Advocates
171 Old Bakery Street
Valletta
Malta

Tel: +356 2123 5406
Email: pmgrimaud@ganadoadvocates.com
URL: www.ganadoadvocates.com

Dr. Paul Micallef Grimaud is a Partner at GANADO Advocates and heads the firm's Intellectual Property, TMT and data protection practice group. Paul's focus is dedicated to counselling and assisting clients in the media, technology and entertainment space, on the legal aspects of their operations, and to representing them in court and arbitration. The team that Paul leads is regularly involved in the drafting and negotiation of IP assignment, licensing and management contracts, advising on content and end-user related matters, registering and enforcing IP rights, and assisting with data protection and regulatory compliance.

Paul is a warranted advocate and regularly represents his clients in arbitration and litigation proceedings relating to intellectual property infringements, anti-counterfeit measures, trade mark and design oppositions, telecoms regulatory matters, media, slander and freedom of information disputes, data protection breaches, and unfair competition cases.

Dr. Luke Hili
GANADO Advocates
171 Old Bakery Street
Valletta
Malta

Tel: +356 2123 5406
Email: lhili@ganadoadvocates.com
URL: www.ganadoadvocates.com

Dr. Luke Hili is an Advocate within GANADO Advocates' Intellectual Property, TMT and data protection practice group. Luke regularly assists clients in relation to various facets of IP protection including, *inter alia*, the registration of trade marks (both nationally and on a EUIPO level) and patents; while also representing clients in litigation proceedings pertaining to the infringement of intellectual property rights and anti-counterfeit measures. In addition, Luke also regularly assists clients with data protection issues including, in particular, the review and/or drafting of the relevant policies required in order to ensure compliance with the General Data Protection Regulation ("**GDPR**").

Besides being involved in the above, Luke also frequently assists clients in disputes relating to carriage of goods in terms of the Convention on the Contract for the International Carriage of Goods by Road ("**CMR**").

GANADO ADVOCATES

GANADO Advocates is a leading commercial law firm with a particular focus on the corporate, financial services and maritime/aviation sectors, predominantly servicing international clients doing business through Malta. The firm also promotes other areas such as tax, pensions, intellectual property, employment and litigation.

The Intellectual Property, Media, Entertainment and Technology practice at GANADO Advocates advises clients on the full range of contentious and non-contentious issues in the technology, media and entertainment space. Services include the registration of trademarks, advice on and drafting of IP agreements, and representing clients in IP infringement lawsuits.

The firm leads a project for the Government of Malta bringing together the various Malta-based legal and advisory service providers with a view to overhauling the current IP legal framework and providing solid and innovative legislative solutions to the IP industries, not least involving blockchain and digital currencies. The team also leads the firm's privacy law practice, assisting all clients on their ongoing GDPR requirements, including data subject requests and investigations by the Information and Data Protection Commissioner. In the media space, the team regularly advises and assists, including through legal representation in Court, key local players on legal matters relating to journalistic freedoms, freedom of information and defamation.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com