Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Malta

Terence Cassar, Ian Gauci and Bernice Saliba
GTG Advocates

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

As a member state of the European Union, Malta's data protection laws include the EU's General Data Protection Regulation (2016/679) (GDPR). Chapter 586 of the Laws of Malta, the Data Protection Act (2018), along with its subsidiary legislation, came into force on 28 May 2018, repealing the previous Data Protection Act of 2001.

Malta is also a party to the Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data (ETS.108), which came into force in 2003.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Office of the Information and Data Protection Commissioner, appointed according to article 11 of the Data Protection Act (2018), is the supervisory authority responsible for overseeing the applicability and enforcement of data protection law in accordance with the requirements of the GDPR.

Further to the provisions of the GDPR and the Data Protection Act (2018), the Commissioner shall have the right to carry out investigations in the form of data protection audits and inspections, as well as demand and access personal data and data processing equipment, records and documentation held by data controllers or data processors. The Commissioner may also request the assistance of the executive police to enter and search any premises in the course of investigation. Moreover, when exercising such investigative powers, the Commissioner may ask for additional information from any person deemed to be of interest; lack of cooperation or the provision of false information may lead to criminal prosecution.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Data Protection Act (2018) provides for joint operations with the supervisory authorities of other EU member states. The Act refers to the GDPR in instances when the national supervisory authority is to cooperate with other supervisory counterparts. In such cases, the Commissioner is to confer his or her powers, including investigative ones, to members and staff of the member states' supervisory authorities; the Act (2018) provides that such conferment of powers is to be made under the exercise and in the presence of the Commissioner.

The GDPR envisages that data protection authorities, referred to as supervisory authorities, provide relevant information and give mutual assistance to other supervisory authorities, thus ensuring that the GDPR is implemented in a consistent manner.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The GDPR provides that administrative fines can be imposed pursuant to its infringement. It is also stipulated that such fines must be effective, proportionate and dissuasive. Supervisory authorities are also instructed to take into consideration several elements when imposing such fines, including but not limited to intent, gravity and degree of cooperation. Different infringements carry different administrative fines.

The Data Protection Act (2018) specifies the administrative fines that can be imposed by the Commissioner by order in writing upon the controller or processor, which fines shall be due to the Commissioner as a civil debt should such persons be found in breach of applicable data protection laws; such fines have not been capped. Fines shall not exceed €25,000 per violation in the case of public authorities or bodies. Moreover, a daily fine can be imposed by the Commissioner for each day on which the violation persists. A €5,000 fine has been imposed on a competent Maltese Authority following a major data breach. A temporary ban on the Authority's online portal was also imposed.

With reference to criminal penalties, the Act (2018) stipulates that if a person knowingly provided false information to the Commissioner or else failed to comply with a lawful request made by the Commissioner during an investigation, that person is to be found guilty of a criminal offence and will be liable to a fine running up to €50,000, with a possible term of imprisonment for six months.

Following the coming into effect of the GDPR, several data breach notifications were made to the Maltese Commissioner, leading to the issuance of a number of fines, which up until April 2019 amounted to nearly €40,000. Most breaches reported were in the financial services sector, followed by breaches in the gaming sector and in public entities. Most of the breaches were reported to be caused by either internal non-malicious action or human error.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Data Protection Act (2018) provides that certain entities, persons and activities are excluded from the scope of the law and consequently the requirements of the General Data Protection Regulation (GDPR). In this case, the Act (2018) follows the provisions of the GDPR when it comes to exempt sectors and institutions. The processing of personal data for activities falling outside of the scope of Union law is excluded; data protection laws also do not apply when the government of Malta carries out activities in accordance with the scope of Chapter 2 of title 5 of the Treaty of the European Union, dealing with common foreign and security policy. Natural persons carrying out personal and household activities are also excluded from the scope of the law. Finally, competent authorities are also excluded from the scope of the law when processing data with the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties, including the safeguarding against and the prevention of threats to public security.

It is also to be noted that the Act (2018) allows certain derogations to be made when processing personal data for scientific, historical, archiving or official statistical purposes. These derogations are only allowed if the full applicability of the law renders the achievement of the exercises in question impossible or impaired and if the data controller believes that such derogations are necessary. In addition, the Act provides that the provisions of the GDPR could be further derogated from in order to exercise the right to freedom of expression and information.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Data Protection Act (2018) itself makes no reference to the interception of communications, electronic marketing or monitoring and surveillance of individuals.

Subsidiary Legislation 586.08, titled 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 and implementing Directive (EU) 2016/680 of the European Parliament and of the Council, addresses technical surveillance, in that it is lawful for competent authorities to collect personal data through technical surveillance or through automated means.

Under Maltese law, Chapter 391 of the Laws of Malta, titled the Security Service Act, addresses the interception of communications, which by the definition provided in the same Act includes an array of activities such as surveillance; the act itself makes no reference to the processing of data. On the other hand, the GDPR addresses direct marketing, but does not distinguish between electronic and non-electronic marketing. In cases of direct marketing, the data subject has the right to object to the processing of their data for marketing purposes.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

Under Maltese law, apart from the Data Protection Act (2018), there are various subsidiary legislations implementing EU regulation or regulations issued by the Minister responsible for data protection.

- Subsidiary Legislation 586.01, titled Processing of Personal Data (Electronic Communications Sector) Regulations and implementing Directive 2002/52 EU of the European Parliament and Council, addresses the processing of data when providing publicly available electronic communications services in public communications networks in Malta and any other country.
- Subsidiary Legislation 586.06, titled Processing of Personal Data for the Purposes of the General Elections Act and the Local Councils Act Regulations, deals with the processing of data in elections held in accordance with Maltese electoral law.
- Subsidiary Legislation 586.07, titled Processing of Personal Data (Education Sector) Regulations, addresses the processing of data by educational institutions and authorities.
- Subsidiary Legislation 586.10, titled Processing of Data Concerning Health for Insurance Purposes Regulations, adds to the existing data protection law when it comes to processing data for insurance purposes and provides for lawful scenarios in which data can be collected.
- Subsidiary Legislation 586.11, titled Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations, provides for the minimum age (currently 13), that minors must have attained for information society services to be able to process the child's data in the absence of parental consent.

PII formats

8 | What forms of PII are covered by the law?

The GDPR lays down rules for the protection of natural persons when their personal data is processed and makes no distinction with regard to its form. The Data Protection Act (2018) upholds the same scope of the GDPR in that data protection law applies to the processing of personal data, wholly or partly, either by automated means or otherwise, where such data is processed to form part of a filing system or is intended for such purpose.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Data Protection Act (2018) mirrors its provisions on the GDPR when defining its territorial scope. The Act is applicable when the processing of data occurs by a data controller (PII owner) or processor in a Maltese establishment. The Act also specifies that processing occurring in a Maltese embassy or in a High Commission situated abroad falls within the scope of the Act. Data controllers or processors not established within the EU are also bound by data protection law if the data subjects being offered goods or services are based in Malta, whether such services or goods are offered for remuneration or free of charge. Data protection law applies if data subjects situated within Malta are being monitored for their behaviour. The provisions of the Act (2018) and the GDPR also apply to data controllers processing data outside of the EU if public international law states that Maltese law is applicable in such circumstances.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The Data Protection Act (2018), along with the GDPR, provides for the establishment of data subject rights and stipulates when such laws are not applicable and when exclusions and derogations apply. Data protection laws apply solely to natural persons. The aforementioned law and regulation differentiate between the role of the data controller and that of the data processor, imposing different responsibilities upon each party.

Under the GDPR, the data controller must maintain documentation recording data processing undertaken by him or her, which shall be available for consultation at any time. Other measures to be taken by the controller include the implementation of and adherence to data protection policies and codes of conduct, adopting a data protection-by-design approach and ensuring that measures to safeguard data are in place through appropriate technical and organisational structures.

With reference to the data processor, the GDPR provides that personal data should only be processed by the processor following the written instructions provided by the controller. When required, a processor must demonstrate their compliance with the GDPR to the controller and supervisory bodies. Unless the controller gives his or her written consent, a processor cannot engage a sub-processor. The processor is obliged to assist the controller with regard to both data subject requests and compliance. If instructed by the controller, a processor should be able to delete data. Moreover, both parties shall cooperate with supervisory bodies and maintain records of the name and contact details of the processor, controller and data protection officer; the purpose of data processing; and the types and categories of data and data subjects in their possession, among others.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 | Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Data Protection Act (2018) relies mainly on the provisions of the General Data Protection Regulation (GDPR), which provide that for the processing of personal data to be lawful:

- the data subject must either have given his or her explicit consent;
- the controller has ensured such data is compliant with a legal obligation; or
- processing is necessary in order to protect the vital interests of the data subjects.

Data processing is also legitimate if it is necessary to carry out a task in the public interest or to fulfil the legitimate interests of the controller, unless such a data controller is a public entity, in which case legitimate interest is not considered to be a legal ground for processing.

Where the processing of data is based on the data subject's consent, the controller shall demonstrate that it was the data subject who freely consented to such processing.

When it comes to the processing of personal data belonging to minors, the GDPR speaks about the consent that can be given by minors to offers of information society services. The GDPR provides that if a minor is under the age of 16, processing of the minor's personal data can only be lawful if authorised by the holder of parental authority. In the case of Malta, the age has been lowered to 13, as allowed by the GDPR, for the purposes of subscription or use of information society services.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

The GDPR prohibits the processing of special categories of personal data, such as data identifying ethnic origin and political opinions or related to health, among others. However, it lays down certain exceptions whereby special categories of data can be processed in accordance with the law of individual member states. Within the remit of Maltese law, the Act (2018) allows for the processing of identity documents, genetic data, biometric data and data concerning health, provided that such processing follows the specific requirements connected to the processing of such special data.

The Processing of Data Regulations for the Education Sector addresses the processing and use of data by educational institutions and authorities.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The Data Protection Act (2018) makes no specific reference to data controllers (owners of personally identifiable information) having to notify individuals whose personal data they hold and relies on the General Data Protection Regulation (GDPR). The latter provides that the data controller may have to communicate with the data subject in cases where the data subject's personal data is rectified or erased. The data controller is also required to notify the data subject should the original processing purposes justifying data collection be changed or expanded and, most importantly, in cases where a data breach has been ascertained and is likely to result in a high risk to the rights and freedoms of the individual. Such notification shall contain a list of the categories and an approximate number of data subjects and data records concerned, the contact details of the controller's data protection officer or alternative representative and the likely consequences and measures taken to address and mitigate the breach.

Within the context of Maltese law, it should also be noted that the Restriction of the Data Protection (Obligations and Rights) Regulations refer to scenarios where data controllers may be required to inform data subjects in cases when their rights are restricted; unless such disclosure is prejudicial for the purpose of the restrictions.

Exemption from notification

14 | When is notice not required?

The data controller shall not be required to notify the data subject of an ascertained data breach where:

- it has implemented appropriate technical and organisational protection measures to the breached data, defusing the risk to the subject's rights and freedoms;
- the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and
- individual notification would require a disproportionate effort.

In such a case, the controller shall instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Control of use

15 Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The GDPR establishes that controllers must inform data subjects of the purposes and legal grounds for processing, including:

- legitimate interest;
- information regarding the recipients or categories of recipients of the data subject's data, if any;
- the intention to transfer the data to a third country or international organisation, if applicable; and
- the period for which the data will be retained.

In cases where processing is based on consent, the data subject shall have the right to withdraw such consent easily, while in cases of processing based upon legitimate interests, the data subject shall have the right to object to such legitimate interests. Furthermore, the GDPR grants the data subject various rights allowing increased control of his or her personal data.

Within the Maltese context, the Restriction of the Data Protection (Obligations and Rights) Regulations provides that when the rights of data subjects are restricted due to the various legitimate reasons provided for by law, the data collected can only be processed for the purpose of its collection, unless the law provides otherwise, or unless the data subject gives his or her consent for the data to be used otherwise.

Data accuracy

16 Does the law impose standards in relation to the quality, currency and accuracy of PII?

The Data Protection Act (2018) makes no reference to the quality, currency or accuracy of personal data and relies on the provisions of the GDPR. The GDPR states that the personal data processed shall be accurate and where possible kept up to date. The data subject is also granted the right to request the rectification of inaccurate personal data; inaccuracy of data gives the data subject the right to restrict the data controller from further processing.

Amount and duration of data holding

17 Does the law restrict the amount of PII that may be held or the length of time it may be held?

While the Data Protection Act (2018) makes no mention of measures regarding minimisation or retention periods with regard to personal data, the GDPR requires the data controller to establish concrete retention periods for all personal data collected, which period shall be notified to the data subject prior to the collection of data. Should such a retention period not be easily determinable, the data controller shall inform the data subject of the criteria to be applied when determining such retention period. The principle of data minimisation requires the data controller to collect only personal data necessary for established processing purposes.

Finality principle

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The GDPR provides that personal data is to be collected for a specified, explicit and legitimate purpose and that if such data is further processed, the processing has to be compatible with the initial purpose of collection. Additional processing may only be conducted following prior notification and provision of information to the data subject.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The Act (2018) acknowledges that in cases of data collected for historical, scientific, statistical and archiving purposes, the same data can be used for other purposes, in which case data controllers and processors must fully abide by the provisions of the Act (2018) and the GDPR.

The Restriction of the Data Protection (Obligations and Rights) Regulations provides that data collected in terms of the parameters of the same regulation can be processed only for the purpose of its collection, unless the law provides otherwise or the data subject gives their consent for the data to be used otherwise.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The General Data Protection Regulation (GDPR) states that personal data is to be processed in an appropriately secure manner. The controller is obliged to include a general description of the technical and organisational security measures taken in its processing activities record. It is also stipulated that both the data controller and the processor are to implement technical and organisational measures to ensure an appropriate measure of security through encryption, pseudonymisation and integrity of the network systems, the creation of data protection policies and codes of conduct, among other measures.

The Restriction of the Data Protection (Obligations and Rights) Regulations also provides that the data controller must implement appropriate technical and organisational measures.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Data Protection Act (2018) makes no specific reference to notifications to supervisory authorities or individuals with regard to data breaches, and relies on the provisions of the GDPR.

The GDPR provides that when there is a personal data breach, the supervisory authority is to be informed by the controller without undue delay and, in any case, within 72 hours of the discovery of the data breach. This period may only be extended in justified cases. In cases where the processor becomes aware of such a breach, the processor must immediately inform the data controller.

In cases of high risk, the breach must also be communicated to the data subject, through direct communication using clear and plain language. The controller may not be obliged to inform the data subject if appropriate technical and organisational protection measures were implemented, subsequent measures to mitigate the breach are taken and if it would involve a disproportionate effort to notify data subjects individually.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The General Data Protection Regulation (GDPR) provides for specific situations where a data protection officer is to be appointed, mainly if:

- the processing is conducted by a public authority, excluding courts acting in their judicial capacity;
- the processing of data occurs on a large scale by controllers and processors whose core activity is data processing; and
- the data controller and processor process special categories of data and data in connection to criminal convictions and offences on a large scale.

The Data Protection Act (2018) stipulates that the minister responsible for data protection can prescribe regulations to designate the mandatory appointment of a data protection officer in cases other than those already provided for by the GDPR.

In terms of the main responsibilities of a data protection officer, the GDPR states that the officer is to inform and advise the controller or processor on their obligations pursuant to the GDPR and other data protection laws, monitor the policies of the controller or processor in relation to the GDPR, cooperate with supervisory authorities and act as a contact point with such an authority, and provide advice on impact assessments. The data protection officer shall also be the point of contact with regard to matters concerning data protection within and outside the organisation.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The Data Protection Act (2018) does not provide for the further keeping of internal records or for the establishment of internal processes or documentation, other than what is provided for in the GDPR. The GDPR provides that controllers shall keep a record of processing activities; processors are also obliged to maintain records of processing activities carried out on behalf of controllers. Both parties shall also maintain documentation relating to the appropriate technical and organisational structures present within their remit in compliance with the GDPR, which shall be available for consultation at any time.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The GDPR requires the application of the principles of data protection by design, which involves the implementation of appropriate measures, controls and processes to ensure data protection principles are adhered to without the need for additional action. Such measures may include pseudonymisation and anonymisation, while adhering to the principles of confidentiality, integrity and availability of personal data. The GDPR also includes the implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

Furthermore, the data controller shall carry out impact assessments where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons; this shall be particularly required in cases where data processing involves the systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, where special category data is processed on a large scale and in cases of large-scale, systematic monitoring of public areas.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

The General Data Protection Regulation (GDPR) and the Data Protection Act (2018) do not require the registration or enrolment of data controllers or data processors with the Office of the Information and Data Protection Commissioner. The Maltese supervisory authority does, however, require the registration and publication of details pertaining to officially appointed data protection officers.

Formalities

26 | What are the formalities for registration?

Not applicable.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

Public access

29 | Is the register publicly available? How can it be accessed?

Not applicable.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

Not applicable.

Other transparency duties

31 | Are there any other public transparency duties?

The Maltese supervisory authority requires the registration and publication of details pertaining to officially appointed data protection officers.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The data controller shall have the right to outsource processing activities to third parties. Such processing must, however, be conducted by appointed data processors guaranteeing compliance with the General Data Protection Regulation (GDPR). Data processors must be appointed in the form of a binding agreement in writing setting out the subject matter and duration of the processing, the nature and purpose of the

processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. The agreement shall include:

- provisions binding the processor to conduct processing activities solely upon the data controller's documented instructions;
- the imposition of confidentiality clauses upon individuals conducting processing activities;
- the implementation of measures aimed at assisting the data controller in complying with data subject requests;
- the implementation of appropriate technical and organisational measures to ensure the security of the personal data being processed;
- the duty to assist data controllers in collaborating and requesting approval from the supervisory authority where necessary; and
- provisions regarding the appointment of sub-processors, which shall only be appointed following the specific or general written authorisation of the controller.

In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

The data processor shall be given clear written instructions with regard to the disposal or return of processed personal data upon termination of the parties' relationship, which methods of disposal or return shall be determined solely by the data controller. The data processor shall also be bound to provide the data controller with all the information necessary to prove compliance with the provisions of the GDPR.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

Cross-border transfers of personal data to third countries or international organisations shall require the Commissioner's authorisations in the absence of an adequacy decision or where the appropriate safeguards to protect data are not in place; such requirement for appropriate safeguards may also be fulfilled through the use of contractual clauses between the parties to the data transfer, as well as through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights, subject to the Commissioner's authorisation. Such transfers shall only be permitted in cases where the proposed transfers are not repetitive, where they concern a limited number of data subjects and where they are required for the pursuit of a data controller's legitimate interest.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The transfer of personal data outside Maltese jurisdiction is not prohibited by the legal regime currently in force and may be affected freely within EU territory, as well as to third countries and international organisations. Transfers of personal data to third-country jurisdictions and international organisations shall take place only in favour of processing entities able to comply with the conditions contained within the GDPR, allowing for adequate protection to data subjects as contained within chapter 5 of the same regulation.

Where the European Commission has determined that a third country or an international organisation offers adequate levels of protection (an adequacy decision), such transfers may take place freely and without the need for specific authorisation; in the absence of such adequacy decisions, the transfer of personal data to a third country or an international organisation shall only be permitted provided that the controller or processor has appropriate safeguards in place and upon condition that enforceable data subject rights and effective legal remedies for data subjects are available in the said third country jurisdiction.

'Appropriate safeguards' include:

- a legally binding and enforceable instrument between public authorities or bodies;
- the application of binding corporate rules;
- the application of standard data protection clauses adopted by the European Commission;
- the application of standard data protection clauses adopted the Maltese supervisory authority and approved by the European Commission;
- the use of an approved code of conduct coupled with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- the presence of an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those necessary for the protection of the rights and freedoms of data subjects.

Without prejudice to the above, the GDPR specifically excludes the transfer of personal data to third country jurisdictions pursuant to court judgments or the decision of a third country administrative authority, unless such request is enforceable by virtue of an international agreement or treaty binding the European Union or Malta and the third country forwarding such request.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Cross-border transfers of personal data to third countries or international organisations shall require the Commissioner's authorisations in the absence of an adequacy decision or where the appropriate safeguards (such as binding corporate rules, standard conractual clauses, etc) are not in place; such requirement for appropriate safeguards may also be fulfilled through the use of contractual clauses between the parties to the data transfer, as well as through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights, subject to the Commissioner's authorisation. Such transfers shall only be permitted in cases where the proposed transfers are not repetitive, where they concern a limited number of data subjects and where they are required for the pursuit of a data controller's legitimate interest.

The transfer of personal data outside Maltese jurisdiction is not prohibited by the legal regime currently in force and may be affected freely within EU territory, as well as to third countries and international organisations. Transfers of personal data to third country jurisdictions and international organisations shall take place only in favour of processing entities able to comply with the conditions contained within the GDPR, allowing for adequate protection to data subjects as contained within chapter 5 of the same regulation.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Onward transfers of personal data from a third country or an international organisation to another third country or another international organisation are subject to the same conditions imposed upon initial transfers to third countries or international organisations.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Article 15(3) of the GDPR grants data subjects the right to request a copy of their personal data being processed by the data controller. Such access shall be provided free of charge and in an easily accessible electronic format should the data subject's request be made by electronic means. Additional copies of that data may also be provided at a reasonable, elective fee covering administration costs incurred by the data controller.

While this access right is generally considered to be universal, it may be lawfully curtailed in particular instances whereby disclosure of personal data may result in the data controller's failure to meet its legal obligations under other laws currently in effect in Malta, such as the Prevention of Money Laundering Act.

Other rights

38 | Do individuals have other substantive rights?

Under the GDPR's provisions, the data subject is also afforded the right to rectification of personal data, the right to erasure of personal data, the right to restrict processing, the right to data portability, the right to object to processing of personal data and the right to lodge a complaint before the relevant supervisory authority with regard to issues relating to the processing of personal data.

The GDPR also prohibits the processing of special categories of personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, save for specific instances or upon the data subject's granting of explicit consent. Furthermore, data subjects have the right not be subjected to decisions based solely on automated decision-making processes, provided that such decisions produce legal effects or other significant effects that may affect the data subject's rights and freedoms.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the provisions of article 30 of the Data Protection Act (2018), data subjects are afforded the right to institute an action for damages against data controllers or data processors processing personal data in contravention of the provisions of the GDPR or of the same Act. The Maltese Civil Courts are empowered to determine the amount of damages representing loss of wages or other earnings, as well as moral damages due to the affected data subject. While claims for damages pursuant to loss of wages or earnings must be necessarily backed by evidence proving mathematically determinable financial losses, claims for moral damages, including injury to feelings, are uncapped and are determined by the civil courts. Such rights to legal remedy shall not preclude the affected data subject from lodging a formal complaint with the Maltese supervisory authority requesting the investigation of alleged breaches of data protection legislation.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Recourse to the right to compensation, representing monetary losses or moral damages, may be exercised personally by affected data subjects through the filing of a sworn application before the First Hall of the Civil Courts of Malta instituting an action for damages against the data controller or data processor processing personal data in contravention of applicable law. Such actions shall be instituted within a period of 12 months from the date when the data subject became aware, or ought to have reasonably become aware, of such a contravention, whichever is the earlier.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The law does not provide for any further exemptions or restrictions.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

The Data Protection Act (2018) establishes the Information and Data Protection Appeals Tribunal, allowing for appeals to be filed against legally binding decisions taken by the Commissioner within 20 days from the service of the Commissioner's decision. The Tribunal shall be composed of a chairperson and two additional members representing the interests of data subjects and of data controllers and data processors respectively. The Tribunal's decisions are furthermore subject to the right of appeal before Malta's Courts of Appeal.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

Subsidiary Legislation 586.01, titled the Processing of Data (Electronic Communications Sector) Regulations, implements the provisions of Directive 2002/52 EC of the European Parliament and Council. The Regulations address the consent required from users before sending unsolicited communication, including SMS and cookies, with the latter being stored on devices.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

The General Data Protection Regulation (GDPR) addresses direct marketing, but does not distinguish between electronic and non-electronic marketing. In the case of direct marketing, the data subject has the right to object to the processing of their data for marketing purposes.

Subsidiary Legislation 586.01, titled the Processing of Data (Electronic Communications Sector) Regulations implementing the provisions of Directive 2002/52 EC of the European Parliament and Council, also provides that a person cannot use electronic communication services to make unsolicited communication for the purpose of

direct marketing by using automated calling machines, emails or faxes. However, the Regulations stipulate that a person may use the contact details obtained from a customer in relation to the sale of a product or a service to directly market its own similar products or services.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The GDPR and the Data Protection Act (2018) do not contain specific provisions regulating the offering of cloud services within the context of data protection and privacy laws; the general principles applied to data processors and data controllers are thus applicable to cloud service providers.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

As the use of technology becomes ever more ubiquitous, and our worlds become ever more connected through various technologies and the eventual rollout of the 'internet of things', matters pertaining to privacy shall increasingly require practical solutions rather than mere reliance on theory. Further developments in big data analytics will push the limits of the General Data Protection Regulation (GDPR) and its applicability. With the collection and storage of personal data, businesses must ensure that the conditions outlined under article 22 of the GDPR, addressing the use of automated individual decision-making and profiling, are adhered to.

When employing the use of big data analytics, businesses shall need to ensure that the consent of the data subject is acquired prior to making use of automated means, unless the use of automated decision making is required to perform a contract between the data subject and data controller or is authorised by European Union or national laws. Profiling of data subjects grants the same data subjects several rights emanating from the GDPR, such as the right to be forgotten and the right to halt certain processes. Although such rights are not absolute, businesses need to ensure that they will be able to take the necessary action upon a request made by the data subject when enforcing their rights.

On another note, the covid-19 pandemic left a certain impact on the global mindset as well as tangible negative economic effects. To this end, there have been certain proposals with a purpose to introduce the use of mobile applications (apps) for contact tracing purposes. While the covid-19 pandemic created a basis for the introduction of such apps, a cautious mindset should be adopted to create a balance between the public interest and the private life of the individual and to ensure that the use of such apps during the pandemic do not create an automatic pretext for future force majeure events .

Dr Terence Cassar
tcassar@gtgadvocates.com

Dr Ian Gauci
igauci@gtgadvocates.com

Dr Bernice Saliba
bsaliba@gtgadvocates.com

66, Old Bakery Street
Valletta
VLT1454
Malta
Tel: +356 2124 2713
Fax: +356 2124 2714
www.gtgadvocates.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7