GUIDANCE NOTE

Malta - Data Transfers

Ian Gauci
GTG ADVOCATES

Terence Cassar
GTG ADVOCATES

Last Updated: May 6, 2026

May 2026

1. Governing Texts

1.1. Legislation

The law regulating data protection and privacy matters in Malta is the Data Protection Act (Chapter 586 of the Laws of Malta) (the Act). As an EU Member State, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) has a direct effect in Malta, and the matters within the GDPR which call for Member State discretion are transposed within the Act.

Prior to the entry into force of the Act and the GDPR, data protection in Malta was regulated under the previous Data Protection Act (Chapter 440 of the Laws of Malta) (the Former Data Protection Act) which has now been repealed and replaced by the Act.

Various pieces of subsidiary legislation have been put into effect under the Act. This body of subsidiary legislation provides for data protection regulation on specific matters. There are currently 11 subsidiary laws, namely:

- Processing of Personal Data (Electronic Communications Sector) Regulations (S.L.586.01);
- Processing of Personal Data (Protection of Minors) Regulations (S.L.586.04);
- Processing of Personal Data for the purposes of the General Elections Act and the Local Councils Act Regulations (S.L.586.06);
- Processing of Personal Data (Education Sector) Regulations (S.L.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 (S.L.586.08);
- Restriction of the Data Protection (Obligations and Rights) Regulations (S.L.586.09) (the Restriction Regulations);
- Processing of Data concerning Health for Insurance Purposes Regulations (S.L.586.10) (the Health Insurance Data Processing Regulations);
- Processing of Child's Personal Data in relation to the Offer of Information Society Services Regulations (S.L.586.11);
- Enforcement of the Rights of Data Subjects in Relation to Transfers of Personal Data to a Third Country or an International Organization Regulations (S.L.586.12);
- Data Protection (Fair Access to and use of Data) Regulations (S.L. 586.13); and
- Artificial Intelligence (Designation of the Information and Data Protection Commissioner for the Purposes of Regulation (EU) 2024/1689) (S.L. 586.14) Regulations.

The Office of the Information and Data Protection Commissioner (IDPC) has also consulted with various sector-specific authorities for the issuance of sector-specific guidance on data protection, such as on data protection in gaming matters (available here).

1.2. Case law

To date of writing, there were only some noteworthy cases that made it in front of an adjudicating body or court, specifically the IDPC in its investigative and decision-making capacity and the Information and Data Protection Appeals Tribunal (the Tribunal), which reviews IDPC decisions at the appeal stage.

In *Allied Newspapers Limited vs. Projects Malta Limited* (Appeal Number 8/2018) (only available in Maltese here), issued on March 26, 2019, the Tribunal (after considering the relevant provisions of both the Act and the Freedom of Information Act (Chapter 496 of the Laws of Malta) (as amended) (the Freedom of Information Act) rejected the appellants appeal from a decision of the IDPC whereby the IDPC rejected the appellant's plea for Projects Malta Limited to disclose a list of names of the members of the Selection Committee that adjudicated on a public tender relating to the management of three public hospitals. The decision delivered by the Tribunal was appealed before the Court of Appeal (Civil, Inferior) (Appeal Number 33/2019) (only available in Maltese here) in accordance with the Act. The Court of Appeal (the Court), in its judgment delivered on September 2, 2020, revoked the decision of the Tribunal, as well as the decision of the IDPC, and ordered Projects Malta to provide the appellant with the names of the members that formed part of the selection committee referred to above without delay.

The Court, after citing various European Court of Human Rights case law in its considerations, based its decision on the fact that, although strictly speaking the names of such persons can be considered to be 'personal data,' the simple disclosure of such names posed no threat to their privacy rights. Contrarily, the Court held that such disclosure was necessary, proportionate, and justified for reasons of substantial public interest in terms of the provision of Article 9 of the Act, and therefore, the exemption relating to documents containing personal data under the Freedom of Information Act did not apply. Additionally, the Court also held that the arguments brought by the respondent that the disclosure of such names would remove the serenity and tranquility necessary to carry out their duties is not valid, firstly on the basis that no safeguards of conflict of interest were put into place for such committee and that the lack of disclosure would render it all the more difficult to become aware of any such conflicts, and secondly, because the lack of disclosure could bring a false sense of serenity and tranquility that could

induce a false belief of also being free from carrying out their duties in a transparent manner. Ultimately, the Court held that one could not argue that the disclosure of such information could prejudice the future supply of information to the Government of Malta (the Government) or other public authority for the purpose of the administration of law or the administration of matters administered by the authority and, therefore, Article 32(1)(c)(ii) of the Freedom of Information Act was not applicable.

The case of *Raymond and Mary Ann Cutajar vs the Commissioner of Information and Data Protection* (Appeal Number 4/2019) (only available in Maltese here) (*Raymond and Mary Ann Cutajar)* issued on October 27, 2020, dealt with data protection considerations and CCTV camera's installed outside an individual's home for surveillance purposes (primarily of a garage). The Tribunal made references to the GDPR, the European Data Protection Board's (EDPB) Guidelines 3/2019 on Processing of Personal Data Through Video Devices, and to the Case C-212/13 *František Ryneš v. Úřad pro ochranu osobních údajů* (Case C-212/13), judgment delivered by the Court of Justice of the European Union (CJEU), to examine the concept of the 'domestic use exemption' and data minimization. The Tribunal reached the conclusion that if the surveillance covers (even partially) public spaces, it cannot be regarded as an activity that is purely a 'personal or household' activity, the appellant does qualify as a 'data controller' in terms of the GDPR, and therefore, is not exempt under such regulation. The Tribunal also examined the concept of legitimate interest, and quoted CJEU Case C–709/18 (only available in Slovak here) that held that 'the legitimate interest needs to be of real existence and must be a present issue.'

Initially, following the coming into force of the Act, a large number of personal data breaches were reported to the IDPC, most of which related to the financial services sector and were caused by internal non-malicious causes. However, the recent trend, not only in Malta, but in most EU Member States, is that the number of data breaches being reported is dropping. In fact, the number of reports to the IDPC between May 2019 and May 2020 dropped from 147 reports to only 97.

More recent notable cases include *LeoVegas Gaming p.l.c vs The Information and Data Protection Commissioner* Appeal Number 161/2018), (only available for download in Maltese here) issued on June 12, 2020, which dealt with the concepts of controller and affiliate marketing in the context of unsolicited

marketing communications by means of affiliate companies. This case was triggered following the UK's Information Commissioner's Office (ICO) request for intervention, as preliminary investigations by the ICO had seemingly revealed various reports filed against the controller in relation to unsolicited text messages. In its ruling, the court confirmed the original IDPC decision and essentially determined that the controller in the relationship between a gaming operator and an affiliate is the gaming operator, and also found that Leo Vegas had failed to provide the required evidence which is necessary to legitimize the sending of the marketing communications by its engaged or appointed affiliates.

Other most recent notable cases include that of *Jan Sammut vs the Commissioner of Information and Data Protection* (Appeal number 15/2019), (only available for download in Maltese here) issued on May 19, 2021, in which a decision was upheld that found HSBC guilty of sharing sensitive personal data without legal basis of one of its employees, after the bank notified through email the Malta Union of Bank Employees that one of its members had been suspended for disciplinary reasons in 2016.

Dorothy Baldacchino et noe v. Carmel D'Amato and Nathalie Spiteri D'Amato, (Appeal number CDP/COMP/319/2021), (only available in Maltese here) issued on June 23, 2022, which is another notable case dealing with data protection considerations and CCTV cameras installed outside an individual's home for the purposes of surveillance. Whilst making reference to the aforementioned *Raymond and Mary Ann Cutajar* case and Case C-212/13. In this case, the Tribunal ruled that a CCTV system overlooking a publicly used but private passageway still does not satisfy the exemption of 'Domestic Use' for the purposes of Article 3(2) of the Data Protection Directive (Directive 95/46/EC).

Case No. CDP/COMP/84/2023 issued on January 9, 2024, concerned article 17 of the GDPR. An individual exercised their right to erasure exercised against an insurance company, who had requested a motor insurance quote but never received such quote from the insurance company, despite engaging in multiple emails, eventually choosing to cease further communication. Frustrated, the individual withdrew their consent for processing and requested that their data to be erased by the insurance company. In reply, the company stated that they have a legal obligation, applicable to the insurance industry to retain data gathered from the

quotation process. Within the investigation by the Tribunal, the company also made reference to retention periods of personal data from quotations which were abandoned, citing the General Data Protection Guidelines: Promotion of Good Practice Insurance Business. The deciding factor in this case was the fact that no quotation was ever given to the individual and thus, on such basis, the Tribunal sided with the individual, finding the company to have infringed on the right to erasure.

Case CDP/COMP/485/2023 issued on January 19, 2024, involved a complaint against a journalist, concerning a claim of illegal and unjustified processing of personal data in a series of hundreds of private WhatsApp messages published on a journalist's personal blog (claimed to have been illegally obtained). The case revolved around the intersection between the notion of a 'private life' and personal data, against the freedom of journalistic expression exemption under Article 9 of the Act. The Tribunal ruled that the controller could have been more faithful to his journalistic freedoms and conducted a thorough assessment by carefully going through all the published messages included in all the published pages of WhatsApp messages in order to identify those chats which were specifically in the substantial public interest to disclose. In order for the exemption of Article 9 of the Act to apply, the processing of such data needs to be i) proportionate, ii) necessary, iii) justified for reasons of substantial public interest, and lastly, iv) strike a fair balance between the right to protection and freedom of expression.

Case CDP/COMP/853/2023 issued on February 2, 2024, involved a complaint before the Tribunal claiming that a police officer hiding out of sight and using a hand-held speed camera breached the right to transparency, as no signage was present to inform the data subjects that they were approaching a zone where their personal data may be processed through a hand-held camera. In reply, the police force presented several arguments, in brief, the force stated that the use of a hand-held speed camera was necessary to determine, beyond a reasonable doubt, whether a driver has committed the offence of over speeding or not. The police force added that the 'capturing' only takes place the moment an offense is committed and that such a system is automated. Most importantly, they argued that there is no law that requires them to post signs of their presence. Having heard both parties, the Tribunal delved into Subsidiary Legislation 586.08 and the *modus operandi* of the police force and having considered the processing, and noting that the EDPB stated that deceptive design patterns would not comply with data protection

principles, the Tribunal ruled that the police were not taking necessary steps to provide any of the necessary transparency information under data protection law by means of a temporary sign placed within a reasonable distance, before the data subjects approach an area where a hand-held speed camera is being used.

Case CDP/COMP/282/2024, issued on April 2, 2025, concerned a complaint against a healthcare provider following its failure to update a patient's residential address, which had been sourced from the local electoral register, ultimately resulting in histopathology reports and other health-related personal data being sent to an outdated address and subsequently disclosed to third parties. In its decision, the IDPC held that the fact that personal data is publicly available through the local electoral register does not grant controllers an automatic right to process such data for purposes beyond those envisaged under the General Elections Act, absent a valid legal basis under Article 6 of the GDPR, nor does it absolve them from complying with the transparency requirements under Article 14 of the GDPR. The IDPC further found that the controller had infringed several provisions of the GDPR, including Articles 14, 16, and 37(1)(c) of the GDPR, particularly in view of its failure to rectify inaccurate data despite repeated notifications and its failure to appoint a data protection officer (DPO) despite processing health data on a large scale. The controller was accordingly reprimanded, ordered to rectify the complainant's data, erase personal data of other data subjects obtained from the electoral register, appoint a DPO, and was further subjected to administrative fines.

Case CDP/COMP/105/2025, issued on December 11, 2025, is a notable case concerning the right of access under Article 15 of the GDPR in a cross-border gaming context. The case arose after a complainant requested from a Malta-established gaming operator an overview of all transactions carried out on their player account. The controller declined to provide the requested data in full, arguing that, pursuant to the German State Treaty on Gambling 2021 (GlüStV 2021), access to gambling transaction data was limited to the 12-month period preceding the request. In its decision, the IDPC rejected that position and held, in substance, that since the controller's main establishment was in Malta, any restriction to the data subject's rights under Article 23 of the GDPR had to be assessed by reference to the GDPR and Maltese law, rather than German law. The IDPC accordingly found an infringement of Article 12(4)

of the GDPR and ordered the controller to provide the complainant with a copy of the full extent of his transaction data undergoing processing.

2. Definitions

Article 3(2) of the Act provides that the definitions provided in the GDPR are directly applicable in Malta and, as such, the key definitions are those found in Article 4 of the GDPR.

Personal data: Any information relating to an identified or identifiable natural person (data subject); 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: 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Data controller: 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; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Data processor: A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

It should be noted that the age of majority for the purposes of consent in the context of information society services is deemed to be 13 years.

3. Scope of Application

The Act applies when:

- the processing of personal data is carried out, wholly or in part, by automated means; and
- the processing of personal data is not carried out by automated means but such personal data forms part of a filing system or is intended to form part of such a filing system.

Nevertheless, the Act provides for several instances when the processing of personal data falls outside of the scope of the Act. These instances mainly relate to:

- an activity which falls outside the scope of EU law;
- activities falling within the scope of Chapter 2 of Title V of the Treaty on European Union carried out by the Government;
- purely personal or household activities by a natural person; and
- preventing, investigating, detecting or prosecuting criminal offenses, or executing of criminal penalties, and safeguarding against and preventing threats to public security by the competent authorities.

The processing of personal data belonging to data subjects present in Malta simultaneously falls within the Act and the GDPR, if such processing is carried out either:

- by controllers or processors not established in the EU in the course of offering goods and services, irrespective of whether payment is involved; or
- in the course of monitoring the behavior of persons present in Malta.

Moreover, processing personal data in the context of the activities of an establishment of a controller or a processor in Malta or in a Maltese Embassy or High Commission abroad, regardless of whether the processing takes place in Malta, falls within the scope of the Act.

If personal data is processed by a controller not established in the EU but who is present in a place where the laws of Malta apply by virtue of public international law, then the Act applies as well.

4. Restrictions on the Transfer of Data

4.1. Within jurisdiction/region

Transfers of personal data within Malta and within the EU may take place without any formality as per the GDPR.

4.2. Outside of jurisdiction/region

The Minister responsible for data protection matters, following consultation with the IDPC, may limit transborder data transfers of specific categories of personal data, both to a third country and to an international organization for reasons of public interest. Such limitation may be imposed in the absence of an adequacy decision (Article 10 of the Act).

The Act makes no other further restriction on the international transfer of data and relies on the safeguards provided for in the GDPR, which (in general terms) requires appropriate safeguards to be implemented data transfers to third countries occur.

5. Data Localization

Data localization requirements are in place in Malta under sector-specific legislation. For instance, the Malta Gaming Authority imposes real-time replication of regulatory data in its Technical Infrastructure Guidelines.

The Malta Financial Services Authority (MFSA) has also imposed, in its Virtual Financial Assets Rulebook (Chapter 3 of the Virtual Financial Assets Rules for

VFA Services Providers), a requirement for license holders to ensure that its IT infrastructure is located in Malta, and/or any other EEA member state, and/or any other third country jurisdiction wherein the Authority is satisfied that the IT infrastructure ensures:

- the integrity and security of any data stored therein;
- availability, traceability, and accessibility of data; and
- privacy and confidentiality.

6. Sector-Specific Restrictions

Health data

Data concerning health is considered a special category of personal data covering both physical and mental health-related personal data and is deemed to capture the same breadth of data captured under the GDPR. In fact, with regard to health data regulation, the Act generally relies on the GDPR, including on the transfers of health data. The main exception in this regard is the Health Insurance Data Processing Regulations, the scope of which is to specifically regulate the processing of data concerning health for insurance purposes, subject to Article 9 of the GDPR.

The Health Insurance Data Processing Regulations provide that the processing of data concerning health must be deemed to be in the substantial public interest when such processing is necessary for the purpose of the business of insurance or insurance distribution activities. Moreover, it holds that such processing must be subject to suitable and specific measures designed to safeguard the fundamental rights and freedoms of data subjects.

Financial data

There are no specific provisions in the Act regulating, in a special manner, the processing of financial data.

The Malta Bankers' Association (MBA), following consultation with the IDPC, issued Data Protection Guidelines for Banks with the purpose of clarifying

parts of the GDPR that are of significance for the banking industry.

Reference should also be made to Restriction Regulations, whereby the rights of data subjects may be restricted when data is being processed for the administration of any tax, duty, fines, fees, and other money due or owed to the Maltese State in terms of Maltese tax law.

HR/employee data

There are no specific provisions in the Act, regulating the processing of human resources or employee data in a different manner to other personal data sets. Accordingly, legitimate interests can be lawful grounds for processing employee data in certain circumstances.

7. Data Transfer Solutions

7.1. Legislative exceptions to the restrictions

The Act adopts the provisions of the GDPR that allow the transfer of data by way of derogations and on certain conditions.

7.2. Usage of data transfer agreements/standard contractual clauses

Entities based in Malta may make use of Standard Contractual Clauses (SCCs) for the purposes of providing appropriate safeguards for international data transfers to third countries. That said, there are practical issues at present in designating Malta as governing law for SCCs since in Malta third-party beneficiary rights are not generally recognized and the designation of governing law to the SCCs which recognizes third-party beneficiary rights is a must under the new version of the SCCs.

Privacy Shield and SCCs in European case law: the Schrems II case

On July 16, 2020, the CJEU published its highly anticipated judgment in Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (the Schrems II Case). In particular, the CJEU declared

the European Commission's (Commission) EU-US Privacy Shield Decision invalid, and, whilst, the CJEU upheld the use of SCCs in principle, it provided clarity around the considerations that organizations and authorities should bear in mind if utilized as the transfer mechanism of choice.

7.3. Usage of intragroup agreements, BCRs, CBPRs

Subject to an approval process, Binding Corporate Rules (BCRs) are recognized and applicable in Malta.

Please note that as a result of the Judgement in the Schrems II Case, the EU-US Privacy Shield was declared invalid. See the section on usage of data transfer agreements above.

7.4. Usage of whitelists and international treaties

Transfers of personal data from Malta to a third country or an international organization may take place where the Commission has issued an adequacy decision. The Commission has the power to issue such decisions that are adopted after notice to and comments from representatives of EU data protection authorities. In a nutshell, an adequacy decision recognizes that a third country awards an adequate level of protection for personal data. If an adequacy decision has been issued and is in force, data exporters do not need to take any further action apart from monitoring that the decision remains valid. Over time, these adequacy decisions have created a whitelist of countries, including Canada, Israel, Japan, New Zealand, and Switzerland. A full list of the Commission's adequacy decisions can be accessed here on the information page regarding adequacy decisions on the official website of the Commission. These adequacy decisions do not cover data exchanges in the law enforcement sector, which are governed by the Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680).

7.5. Other solutions

The Act relies on the GDPR, specifically Article 46, whereby data can be transferred subject to appropriate safeguards.

7.6. Notification/approval requirements for the above

Notification to the IDPC is required where modified SCCs are used for the purpose of third-country transfers and for the use of BCRs.

8. Sanctions

With respect to the private sector, the applicable sanctions are those set out within Articles 83 and 84 of the GDPR.

On the other hand, with respect to the public sector, the IDPC is empowered to impose administrative fines on public authorities and bodies, which do not exceed the amount of €25,000 for each given violation and an additional daily €25 fine which may be imposed if the violation persists. Furthermore, for intentional or negligent infringements of public authority or body acting, the IDPC may impose a fine which does not exceed the amount of €50,000 for each given violation, whereby an additional daily €50 fine may be imposed if the violation persists.

Additionally, Article 22 of the Act stipulates that any person who knowingly gives false information to the IDPC or does not comply with any lawful requests by the IDPC must be liable to pay a minimum €1,250, but not more than €50,000, and may even face imprisonment for up to six months.

Topics: Data Transfers

Jurisdictions: Malta