The national funding agency (FNR) does not support data protection efforts with any tools or guidelines. The Luxembourg Agency for Research Integrity provides some basic introductions into data protection rules. The Code of Conduct for Scientific Research will provide comprehensive tools once finalised. However, this effort is pursued by the research stakeholders and supported by Ministry of Higher Education and Research directly.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

Not to our knowledge.

19 Malta

Aitana Radu (University of Malta)

19.1 Informed consent

19.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Data Protection Act (Cap 586)	https://idpc.org.mt/en/Legislation/CAP%20586.pdf	Hard law	The Maltese Data Protection Act was amended in April 2018 (by repealing and replacing the Data Protection Act, Cap 440) to reflect the changes brought about by the General Data Protection Regulation (GDPR). The GDPR's regulatory scope is far wider than the original Data Protection Act (DPA).
SL 586.01 Processing of Personal Data (Electronic Communications Sector) Regulations	https://idpc.org.mt/en/Legislation/SL%20586.01.pdf	Hard law	Date in force: 15th July, 2003. It implements 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. A distinctive element in Maltese legislation can be seen in the Electronic Communications Regulations, namely Article 9, which addresses unsolicited communications for the purposes of direct marketing. The general rule is that such communications, including

			communications made by means of an automatic calling machine, a facsimile machine or email, whether to a natural or legal person, require prior consent in writing. This general rule, however, contains an exception. Where a person has obtained, from his customers, their email contact details in relation to the sale of a product or service which had been requested by the customer, such person can use their details for direct marketing of its own similar products or services. In such a case, however, the customers must be given the opportunity to opt out, free of charge and in an easy and simple manner, at the time of the collection as well as in each message, in the case where the customer did not initially opt out.
SL 586.04 Processing of Personal Data (Protection of Minors) Regulations	https://idpc.org.mt/en/Legislation/SL%20586.04.pdf	Hard law	Date in force: 12th March, 2004. It deals with the processing of personal data of minors by schools, authorities of legal guardians for the protection of the minors. The Protection of Minors Regulations state that where any information is derived by any teacher, member of a school administration, or any other person acting instead of the parents of the child, or in a professional capacity, in relation to a minor, such information may be processed as follows, as long as the processing is in the best interest of the minor: • where personal data is being processed as aforementioned, the consent by the parents or other legal guardian of the minor shall be not be required if this may be prejudicial to the best interest of the minor; • with respect to the above, no parent or legal guardian of the minor shall have access to any personal data held in relation to such minor. Pursuant to Article 8 of the GDPR, the Processing of Child's Personal Data in Relation to the Offer of Information

			Society Services Regulations state that processing of personal data of a child in relation to information society services shall be lawful where the child is 13 years of age.
SL 586.07 Processing of Personal Data (Education Sector) Regulations	https://idpc.org.mt/en/Legislation/SL%20586.07.pdf	Hard law	Date in force: 09th January 2015. It deals with the processing of personal data by educational institutions and authorities in Malta.
SL 586.08 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	https://idpc.org.mt/en/Legislation/SL%20586.08.pdf	Hard law	Date in force: 28th May 2018. These regulations transpose Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the 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, and on the free movement of such data. Where a controller processes special category data in the public interest, the controller shall consult with and obtain prior authorisation from the IDPC, where the data processed is: • genetic data, biometric data or data concerning health for statistical or research purposes; • special categories of data in relation to the management of social care services and systems, including for the purpose of quality control, management information and the general national supervision and monitoring of such services and systems. Where genetic data, biometric data or data concerning health are required to be processed for research purposes, the IDPC shall consult an ethics committee or an institution recognised by the IDPC. With reference to the processing of criminal conviction data, the Malta Police Force keeps a register of criminal

			convictions. Police conduct certificates are issued solely by the Commissioner of Police, at the request of the data subject or upon a Court order given ex-officio, or at the request of an interested party. Data of criminal convictions may also be disclosed to other national competent authorities as required by law or with the explicit consent of the data subject. Having said this, judgements of the criminal courts of Malta are available to the general public.
SL 586.09 Restriction of the Data Protection (Obligations and Rights) Regulations	https://idpc.org.mt/en/Legislation/SL%20586.09.pdf	Hard law	Date in force: 1st June 2018. Pursuant to Article 23 of the GDPR, these regulations introduce restrictions on some data subject rights and obligations where this is necessary for: national security; the prevention or detection of criminal offences; or tax-related matters.
SL 586.10 Processing of Data concerning Health for Insurance Purposes Regulations	https://idpc.org.mt/en/Legislation/SL%20586.10.pdf	Hard law	Date in force: 1st June 2018. These add 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. Processing health data is permitted where: • such processing is necessary and proportionate in the context of a policy in the business of insurance; For instance, this derogation may be applied in circumstances where data concerning health is deemed necessary to settle insurance claims.
SL 586.11 Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations	https://idpc.org.mt/en/Legislation/SL%20586.11.pdf	Hard law	Date into force: 1st June 2018. The legislature has clarified that in the absence of consent from a child's parent or legal guardian, the processing of a child's personal data in relation to information society services will be lawful only for children that are 13 years old or older. This does not alter the rules on the age of consent for entering into contracts, as that is separately governed by Maltese law.
SL 586.06 Processing of Personal Data for the	https://idpc.org.mt/en/Legislation/SL%20586.06.pdf	Hard law	Date into force: 18 January 2013. Personal data, including sensitive personal data, may be processed by any person entitled to do so for the purpose of implementing

Purposes of the General Elections Act and the Local Councils Act Regulations			the General Elections Act and Local Councils Act.

Main regulatory tools addressing data protection issues and informed consent in Malta

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

Natural persons carrying out personal and household activities are excluded from the scope of the Data Protection Act (Cap 586) and there is no other legislation covering these data categories.

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

National security is another area which is excluded from the scope of the Data Protection Act (Cap 586). 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. However, the act itself makes no reference to the processing of data.

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.

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
The Information and Data Protection Commission ('IDPC') is the national supervisory authority and is appointed in accordance with Article 11 of the Data Protection Act	https://idpc.org.mt/en/Pages/Home.aspx	Yes	Est. 16 people	High	In 2018 there were 25 public presentations, 520 one-to-one meetings with controllers, 76 complaints investigated and 18 fines issued).

Information regarding Data Protection Authority, Malta

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

The Data Protection Act (Chapter 586) contains special rules relating to the processing of personal data for journalistic, research, archiving, historical and statistical purposes. While, there is no specific definition of "data processing for research purposes", there are specific provisions regarding this type of activity as explained below.

Where processing is carried out for the purposes of archiving in the public interest, scientific or historical research purposes or official statistical purposes, the rights of data subjects under Arts. 15-6, 18 & 21 GDPR do not apply, to the extent that the exercise of such rights would likely render impossible or seriously impair the achievement of such purposes, and the controller reasonably believes that it is necessary for the fulfilment of such purposes. Where such data processing serves another purpose simultaneously, the derogations will apply only to processing for the aforementioned purposes.

Another specificity in Maltese legislation is related to health data (Processing of Personal Data (Secondary Processing) (Health Sector) Regulations (S.L. 528.10 of the Laws of Malta. Date into force: 8th of October 2019)). The Regulations provide that health data can be processed for research activities which are in the public interest. In the case of research activity conducted by the Ministry of Health or its partners, such research can be carried out following approval of the Health Ethics Committee within the Ministry of Health and after obtaining prior authorisation from the IDPC; in the case of research activity conducted by academics or students or NGOs having the remit to assist patients in need in the health sector, such research can be carried out following approval of any other ethics committee recognized by the IDPC and after obtaining prior authorisation by the IDPC. In such cases personal data must be pseudonymised, however if this also not possible, appropriate measures should be taken to safeguard the rights and freedoms of data subjects by ensuring that the personal data is anonymised as soon as it is no longer required in an identifiable manner for the purpose of carrying out research or statistical studies.

The IPDC has also published a set of guidelines covering this area, which are available at https://idpc.org.mt/en/Documents/DPCresearchguidelines.pdf.

(v) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

Data processing for research purposes must be subject to appropriate safeguards protecting the rights and freedoms of the data subject, including pseudonymisation and other technical and organisational measures to ensure respect for the principle of data minimisation. Where such purposes can be achieved by processing which does not permit, or no longer permits, the identification of data subjects, those purposes must be fulfilled in that manner (art 6 of Chapter 586).

Maltese legislation includes provisions for processing sensitive data beyond article 9 of the GDPR, namely personal, including sensitive personal data, may be processed by any person entitled to do so for the purpose of implementing the General Elections Act and Local Councils Act.

In addition to this Maltese Subsidiary Legislation 586.10 regulates the processing of data concerning health for insurance purposes. Among other things, these regulations stipulate that the processing of data concerning health shall be lawful where such processing is necessary and proportionate for the purposes of a policy in the business of insurance, where the data controller cannot reasonably be expected to obtain the consent of the data subject, and where the data controller is not aware that the data subject is withholding consent.

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

There are no such Codes at a national level, however the University of Malta, which is the only public higher education institution in the country has two such documents: The University's Research Code of Practice (https://www.um.edu.mt/__data/assets/pdf_file/0011/338942/ResearchCodeofPractice.pdf) and the University's Research Ethics Review Procedures.

The University's Research Code of Practice states that all research carried out at the University should recognise the rights of individuals to privacy and personal data protection and honour the requirement of informed consent and continuous dialogue with research participants. Furthermore, it provides clear guidelines on obtaining consent from research participants.

The University's Research Ethics Review Procedures provides detailed information on the bodies handling ethical issues within the University and the steps which need to be followed by researchers. It is relevant to mention that the University's Research Ethics Committee (UREC) has a dedicated sub-committee for data protection (UREC-DP).

The role of UREC-DP is to: (a) Liaise with the Malta Information and Data Protection Commissioner (IDPC) in terms of Section 7 of Chapter 586 of the Laws of Malta (Data Protection Act 2018) to obtain any necessary authorisation required for research proposals that have been referred to it; (b) Review research proposals, referred to it by the Faculty Research Ethics Committees (FRECs), that deal with special categories of personal data as defined in the GDPR; (c) Carry out annual audits of research data protection self-assessments carried out by Researchers and reviews carried out by FRECs on data protection matters not related to special categories of personal data to ascertain that self-assessments and reviews are consistent with the policies approved by Senate, the GDPR, and Chapter 586 of the Laws of Malta (Data Protection Act 2018); (d) Prepare an annual report to Senate summarizing activities carried out, including the results of the audit; (e) Arbitrate in those cases where Researchers do not agree with FREC decisions on data protection matters not related to special categories of personal data; and (f) Prepare recommendations to Senate for improvement of Research Data Protection policies or procedures that deal with data protection

(vii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

There is no specific definition in Maltese legislation of data processing for “statistical purposes”. There is, though, a definition for "official statistics", which are designed as “information collected, analysed and produced for the benefit of the society to characterize collective phenomena in a considered population and produced by the National Statistics Office as provided for by law, or by other national authorities as designated by Eurostat following recommendation by the National Statistics Office.”

In the case of sensitive data processed for the compilation of statistics, this would in principle only be permitted with the explicit consent of participants. However, where similar statistics are necessary in the public interest, such statistics may be collected subject to the direct approval of the Commissioner himself.

(viii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

Where personal data is used for university related research, the Act does not require the specific approval of the Data Protection Commissioner, unless such information involves sensitive data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life. If one of the abovementioned categories is processed, the Act stipulates that similar research requires the approval of the Commissioner upon advice from a research ethics committee recognised for such purposes. The Commissioner recognises the University Research Ethics Committee (UREC) as his advisory body entrusted to approve university related research involving sensitive data. Given that every project involving human subjects always requires an ethical approval from UREC, the Commissioner reached an agreement whereby UREC approves projects both in terms of ethical and data protection considerations in order to speed up the research process. Such approval is granted on the condition that the researcher abides by the necessary data protection requirements which are contained in the application form submitted by the researcher. Research projects are primarily evaluated by the respective faculty research ethics committee and then if the application fulfils the necessary criteria, this is forwarded to UREC for approval. Where in the evaluation of specific projects, there is uncertainty on complex data protection issues the Commissioner is always consulted.

19.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

(ii) Are there any special requirements regarding informed consent at the national level?

(iii) Are there any special requirements regarding data processing at the national level?

(iv) Are there any special requirements to exercise data subject’s rights (right of access, correction, deletion of personal data)?

There are no particularities regarding data subjects at national level.

There are no special requirements regarding informed consent at national level.

In terms of special provisions regarding data processing, the Data Protection Act makes provisions for the processing of personal data relating to the purpose of exercising the

right to freedom of expression and information, including provisions for the processing of data for journalistic purposes or for the purposes of academic, artistic or literary expression, wherein these shall be exempt from compliance with select provisions of the GDPR. These exemptions only apply in cases where in reconciling the right to protection of personal data and the right to freedom of expression, the controller has ensured that the processing is proportionate, necessary and justified for reasons of public interest.

In terms of exercising data subject's rights, according to Maltese legislation, controllers and processors may derogate from the right of information to be provided in relation to the processing of personal data for scientific and historical research purposes, official statistics and archiving purposes in the public interest, in so far as the exercise of the rights set out in the right of information to be provided:

- is likely to render impossible or seriously impair the achievement of those purposes; and;
- the data controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.

Processing for the aforementioned purpose shall be subject to safeguards for the rights and freedoms of the data subject, including pseudonymisation and other technical and organisational measures to ensure respect for the principle of data minimisation. Where these purposes can be fulfilled by processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

19.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

(iii) Are there other vulnerable individuals identified in your national legislation?

Maltese legislation includes provisions for processing sensitive data beyond article 9 of the GDPR, namely personal, including sensitive personal data, may be processed by any person entitled to do so for the purpose of implementing the General Elections Act and Local Councils Act.

When it comes to the processing of personal data of children, there are no special rules. The age for consent will depend on the type of processing activity:

- 13 years of age for processing by or on behalf of information society services; and
- 16 years of age for processing personal data of students.

There are no other categories of vulnerable individuals identified in the legislation

19.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

There are no specific rules governing this issue

19.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

In Malta, the Information and Data Protection Commissioner has the power to draw up a list of "high risk" processing activities which would be subject to an impact assessment.

The IDPC established the following processing operations where a Data Protection Impact Assessment ('DPIA') must be carried out by controllers prior to the processing. The list has been compiled after considering the guidelines on DPIAs that were adopted by the WP29, and subsequently endorsed by the European Data Protection Board ('EDPB'). The list is non exhaustive and is as follows:

- Systematic monitoring: personal data that involves:

o observing, monitoring or controlling data subjects' behaviour, in particular, on the online environment;

o specific circumstances where the controller is legally required to process personal data about data subjects without their knowledge;

o operations concerning the use of geolocation data, including but not limited to, for the purpose of direct marketing; or

o monitoring on a large scale of public spaces or private areas accessible by the public.

- Automated decisions: fully or partially by means of processing, including profiling, which produces legal effects concerning the data subjects or similarly significantly affects them.

- Use of innovative technologies: any processing of special categories of personal data and of data concerning vulnerable data subjects, using innovative technologies or the implementation of new methods in existing technology.

- Special categories of data: processing on a large scale of special categories of data, including, personal data relating to criminal convictions and offences.

- Biometric data: any processing activity involving biometric data for the purposes of uniquely identifying data subjects:

o when the data subjects are in a public space or in a private area accessible to the public;

o when the biometric data are processed in conjunction with personal data related to criminal convictions and offences;

o when the biometrics are related to individuals who need high protection such as minors, employees, patients, mentally ill persons and asylum seekers.

- Genetic data: any processing of genetic data, other than that processed by an individual health care professional when providing a related service directly to the data

subjects, for the purpose of matching or combining data sets in a way that would exceed the reasonable expectation of the data subject.

- Data concerning vulnerable persons: processing of personal data of vulnerable natural persons, in particular, concerning children, employees and individuals receiving any form of social assistance;

- Employee monitoring: processing of personal data for the purpose of the evaluation or scoring of aspects concerning the employee's performance at work, or when the processing increases the power imbalance between the data subjects and the data controller, particularly, when the employees may be unable to easily consent to, or oppose, the processing of their data or exercise their rights.

- DPIAs are not subject to the authorisation of the Commissioner. The controller shall only consult the IDPC prior to processing when, notwithstanding reasonable mitigating measures taken in terms of available technologies to address the high risks following the carrying out of the DPIA, residual risks would still be present in the processing operation. The controller must also consult and obtain prior authorisation from the IDPC where the controller intends to process the following data in the public interest:

o genetic data, biometric data or data concerning health for statistical purposes (the IDPC will consult a research ethics committee or an institution recognised by the IDPC); or

o special categories of data in relation to the management of social care services and systems, including for the purposes of quality control, management information and the general national supervision and monitoring of such services and systems.

19.2 Commercialization of data

19.2.1 General Regulatory Framework

There are no rules on data commercialization as such in Malta.

19.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

(ii) Do you know if these practices are routinely performed?

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

In practice, there are contracts based on exchange of personal data for services. It is difficult to assess how often are these practices.

There are no specific regulations on the remuneration of data subjects if profit is made out of their data.

(iv) Do you have any particular national regulation on the secondary use of data?

There are, however regulations regarding the secondary use of data. One such example are Processing of Personal Data (Secondary Processing) (Health Sector) Regulations (S.L. 528.10 of the Laws of Malta). The purpose of the Regulations is to permit certain secondary processing of personal data in the health sector, effectively allowing the

processing of health data for purposes other than those for which the personal data was initially collected for in certain cases by health care professionals. Such secondary health data processing may be allowed for specific cases, mainly:

- for the processing and analysis of records by licensed entities within the health sector for the purpose of managing and enhancing health services;
- for the analysis of health records, as supplied by the Ministry for Health, for the purpose of monitoring and ensuring the quality and cost effectiveness of the health service;
- for the monitoring of contractual obligations, for quality control and for the management of information and monitoring of services and systems arising from public-private partnerships and partnerships with non-governmental organisations ("NGO"). Moreover, secondary processing is also allowed for the purposes of ensuring adherence to contractual obligations and the delivery of a safe and accessible service;
- to fulfil obligations related to the provision of statistical information;
- for the compilation of evidence in medico-legal cases;
- for the investigation and monitoring of health threats; and
- to access health records for research activities.

(v) Do you have any specific protection for metadata or non-personal data in your country?

There are no specific legislative protections for metadata or non-personal data. However, these issues are addressed in the National Data Strategy (https://www.mita.gov.mt/en/nationaldatastrategy/Pages/National-Data-Strategy.aspx)

19.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

There is no official classification of data in Maltese legislation. However, the National Data Strategy published by the Malta Information Technology Agency in 2016 mentions the plans for a comprehensive data classification scheme which will cover the main aspects of enterprise data management (https://mita.gov.mt/en/nationaldatastrategy/Pages/National-Data-Strategy.aspx).

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Copyright is covered by the Copyright Act (Chapter 415 of the Laws of Malta). Infringement of copyright in Malta leads to exposure from both a civil and criminal perspective. Under the Criminal Code (Chapter 9 of the Laws of Malta), copyright infringement carries both the possibility of fines as well as imprisonment. From a civil perspective, cases are litigated before the First Hall of the Civil Court at first instance. Increasingly, the Maltese courts are also recognizing damages not just for material and actual damages but also for moral damages

Under the Enforcement of Intellectual Property Rights (Regulation) Act, an injured party can request the court to order the infringer to pay damages commensurate with the actual prejudice suffered as a result of the infringement. When calculating the amount of damages due, the court takes account of all relevant aspects, including: the negative economic consequences suffered (such as loss of profits); any unfair profits made by the infringer.

The law also provides an alternative method of calculation of the amount of damages due, where a lump sum of damages payable is set by the court by reference to, among other things, the amount of royalties or fees that would have otherwise been due had the infringer requested authorisation to use the right concerned. However, in cases where there is a lack of knowledge on the part of the infringer, the court may determine the amount to be paid by the infringer by applying pre-established practices concerning the quantification of amounts of recovery of profits or payment of damages.

19.3 Security and cybersecurity

19.3.1 General Regulatory Framework

Regulation	Link	Type of regulation (hard law, soft law)	Brief description and scope
Maltese Criminal Code provisions dealing with cybercrime under sub-title V 'Of Computer Misuse'	http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574&l=1	Hard law	Within the context of Maltese jurisdiction, Article 337 of the Criminal Code, identifies computer misuse under various forms including: unlawful access to information; unlawful use of information; misuse of computer hardware; misrepresentation of another person; and unauthorised copy of software and supporting documentation.
Processing of Personal Data (Electronic Communications Sector) Regulations (SL 586.01)	http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=11052&l=1	Hard law	Date in force: 15th July, 2003. It implements 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.

			The Processing of Data Regulation 20 establishes that services providers must retain certain categories of data necessary to: • trace and identify the source of a communication; • identify the destination of a communication; • identify the date, time and duration of a communication; • identify the type of communication; • identify users' communication equipment or what purports to be their equipment; and • identify the location of mobile communication equipment.
Electronic Communications Networks and Services (General) Regulations (SL 399.28)	http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=10563&l=1	Hard law	Date into force: 12th July 2011. The Electronic Communications Networks and Services (General) Regulations (S.L. 399.28), on the other hand, requires undertakings which provide publicly available electronic communications services to inform subscribers and users (where possible) about the existence of any situations allowing the contents of communications to be unintentionally made known to persons who are not party to them. It also covers industry-specific considerations such as the obligation of telecoms undertakings to provide users

			with simple and free of charge solutions for the prevention of calling-line identification, preventing the presentation of the calling line identification of incoming calls and the rejection of incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber, and stopping automatic call forwarding by a third party to the terminal of that subscriber's without delay. Such calling line identification prevention may be overridden when a subscriber requests the tracing of malicious or nuisance calls received on his/ her line or where the undertaking deems it necessary or expedient to trace any such calls.
Council of Europe Cybercrime Convention			Malta has been a signatory since 2001, and which was ratified in April 2012

Main regulatory tools addressing security and cybersecurity in Malta

19.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The transposition document of Directive (EU) 1148 of 2016 - the NIS Directive, was approved by the Cabinet of Ministers in Malta. The Legal Notice, namely L.N. 216 of 2018 on "Measures For High Common Level of Security of Network and Information Systems Order, 2018" was published and it is available here http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29161&l=1

The National Competent Authority and Single Point of Contact in Malta is the Critical Information Infrastructure Protection Unit (CIIP Unit) within the Malta CIP Directorate and the National CSIRT in Malta is CSIRT Malta.

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

There are only generic requirements under applicable legislation relating to cybersecurity, which state that the security of systems must be adequate in relation to the sensitivity of information and repercussions that may arise as a result of information security breaches. There are no explicit or specific legislative requirements in addition to the above.

However, companies that are obliged to maintain adequate security in their business (such as financial services, telecoms, remote gaming) and normally have to undergo supervisory checks by their licensing authorities normally adopt ISO 27001 standard. Moreover, financial service providers having to undergo PCI compliance generally follow the applicable rules as well with regard to the storing of data and its encryption.

19.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

The Data Protection Act 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 Electronic Communications Networks and Services (General) Regulations (Subsidiary Legislation 399.28) provide that where there is a significant risk of a breach of security or integrity of the services or network, the provider must appropriately, and without undue delay, notify any users concerned of the possible risks and remedies available, as well as contact points for more information. Where the Communications Authority – the authority responsible for network security in Malta – determines that the network security breach is in the public interest, it may inform the public or require the undertaking concerned to do so accordingly.

The Financial Services Authority similarly imposes a duty on financial institutions to report immediately any security breaches to it, the Maltese Central Bank and, in the event of a personal data breach, the Office of the Information and Data Protection Commissioner. Operators in the investment services and insurance fields are subject to similar duties, whether in the form of licence conditions or by regulation.

In the remote gaming sector, the Gaming Authority requires operators to report any breaches or attacks on their systems. These reports need to be prepared in the form of a prescribed incident report form and submitted to the Gaming Authority within 24 hours of the relevant incident.

19.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or

something similar established? If yes, what are the competences and responsibilities?

There is no such one authority supervising cybersecurity. The regulation and enforcement of cybersecurity aspects is however addressed by several different agencies:

- The Office of the Information and Data Protection Commissioner is empowered to regulate and enforce cybersecurity aspects of personal data processing.
- The Communications Authority is the authority responsible for enforcing the security of Malta's public communication networks.
- The Maltese police are responsible for detecting, investigating and prosecuting cybercriminals, primarily through a specialised team – the Cyber Crime Unit.
- Other industry-specific authorities, such as the Financial Service Authority and the Gaming Authority, are the relevant authorities to report to for operators holding licences issued by such authorities.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

Insurance coverage for cybersecurity is available for companies in Malta. Moreover, private parties may seek private redress under the provisions of the Civil Code.

However, these issues are not sufficiently regulated.

In what regards data breaches, a data subject may, by way of an application filed before the court, exercise an action for damages against any data controller who processes data in contravention of the Data Protection Act. Such action must be instituted by the data subject within 12 months from the date on which he or she becomes aware or could have become aware of the circumstances causing the damage. While there is no specific provision on the size of damages that may be awarded for a breach of a data subject's rights, the basic principles of Maltese tort law would require the data subject to prove the value of actual damages suffered and any lost earnings caused by such a breach.

19.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

(ii) Are there administrative fines related to data protection issues?

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

The Data Protection Act provides that any person who knowingly provides false information to the commissioner or does not comply with any lawful request pursuant to an investigation by the commissioner will be guilty of an offence. Any conviction will result in a fine of no less than €1,250 and no more than €50,000, imprisonment for six months or both. DPOs of a company should be vigilant in this regard, as this implies personal criminal liability.

In what concerns administrative fines related to data protection issues, the IDPC has the power to impose such fines on a public or government authority. However, depending on the nature of infringement, these fines will be capped at:

- €25,000 for each violation and a possible daily fine of €25 for each day during which such violation persists; or
- €50,000 for each violation and a possible daily fine of €50 for each day during which such violation persists.

Data protection offences are official offences in Malta.

19.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

All research carried out by the University of Malta is subjected to ethical review. This is regulated by the University's Research Code of Practice and the University's Research Ethics Review Procedures

The review procedures start with the researcher completing a self-assessment exercise on Research Ethics and Data Protection (REDP) . Depending on the outcome of this self-assessment, the researcher may either commence the research or apply for REDP Review to the Faculty's Review Ethics Committee (FREC) .

FRECs are authorised to review and approve REDP review applications on behalf of the University, that are not automatically approved through the self-assessment process, except (a) if the proposed research involves special categories of personal data (SCPD) as defined in EU Regulation 2016/679, General Data Protection Regulation (GDPR), and (b) where ethics or data protection issues cannot be resolved with the researcher. In these instances, the FREC shall review the application for any ethics considerations and make a recommendation to the University's Research Ethics Committee.

The University's Research Ethics Committee has two streams: an Ethics stream and a Data Protection stream.

The role of UREC-E is to audit research ethics self-assessment and ethical reviews carried out by FRECs.

The role of UREC-DP is to:

- liaise with the Malta Information and Data Protection Commissioner (IDPC) in terms of Section 7 of Chapter 586 of the Laws of Malta (Data Protection Act 2018) to obtain any necessary authorisation required for research proposals that have been referred to it;
- review research proposals, referred to it by the FRECs, that deal with special categories of personal data as defined in the GDPR.;
- carry out annual audits of research data protection self-assessments carried out by Researchers and reviews carried out by FRECs on data protection matters not related to special categories of personal data to ascertain that self-assessments and reviews are consistent with the policies approved by Senate, the GDPR, and Chapter 586 of the Laws of Malta (Data Protection Act 2018); (d)Prepare an annual report to Senate summarizing activities carried out, including the results of the audit.

There are no specific provisions in the Research Code on R&I activities related to dual use or security-sensitive technologies.

20 Netherlands

Ernst Halberstadt (Independent researcher)

20.1 Informed consent

20.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Grondwet (Constitution)	https://wetten.overheid.nl/BWBR0001840/2018-12-21	Constitution	art. 10 enshrines the constitutional right to privacy and data protection
Algemene Verordening Gegevensbescherming (AVG/GDPR)	https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679	Hard law	Directly applicable in the Netherlands. Supersedes Wet bescherming persoonsgegevens (Wbp) which was the national implementation of the Privacy and Data Protection Directive '95