14 Ireland

Oliver Feeney (University College Cork)

14.1 Informed consent

14.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Data Protection Act 2018 (Revised 2019)	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html http://revisedacts.lawreform.ie/eli/2018/act/7/revised/en/html (revised 2019)	Hard law	As an EU Regulation with 'direct effect', GDPR did not necessarily require transposition into Irish law, but nevertheless the Data Protection Act 2018 was signed into Irish law on 24 May 2018 to give the Regulation national effect. *[Aside note: Throughout, unless otherwise explicitly stated, the following information on Ireland refers to the Republic of Ireland. While a devolved assembly and power-sharing arrangements exist for Northern Ireland, Northern Ireland is under the jurisdiction of the United Kingdom]* The 2018 Act changed the previous data protection framework, established under the Data Protection Acts 1988 and 2003. The key aspects of the 2018 Act include: > Transposing the Directive's legal requirements into Ireland's national law. > The 2018 Act established a new Data Protection Commission as the State's national independent data protection authority responsible for upholding the personal data protection rights specified by the GDPR. The Commission is Ireland's supervisory authority with responsibility for monitoring the application of the GDPR. In addition, the Commission also has certain functions with regard to the Irish ePrivacy Regulations (2011) and the EU Law Enforcement Directive. The Commission is headed by Helen Dixon (Commissioner for Data Protection). > It also gives further effect to the GDPR in areas where Member States have some

			flexibility such as setting the digital age of consent. Under this lee-way, the Irish Parliament has set the digital age at 16 in an amendment to the Data Protection Bill. > [**Data protection for research purposes under GDPR**] A person proposing to process personal data for health research purposes requires the explicit consent of any individual (data subject) whose data he or she is proposing to process and in order that such consent should be valid and lawful it must be (a) informed and (b) appropriately recorded (thereby making it explicit). Consent is defined in Article 4 of the General Data Protection Regulation (GDPR), which in turn defines the parameters of the Irish Department of Health guidance on informed consent for the data subject, which states that it be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/Health_Research_Information_Principles.pdf
The Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019 (S.I. No. 188 of 2019).	http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf	Hard	The Data Protection Act 2018 research-related provisions are given further and more specific effect through the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018. They outline the mandatory appropriate and specific measures for the processing of personal data for the purposes of health research, while providing a definition of health research for the purposes of the regulations, as well as providing for the possibility of applying for a consent declaration for new research (incl. transitional arrangements for health research that is already underway). The Regulations also provide for the establishment of a committee tasked with making on applications for consent declarations and appeals

Disability Act 2005	http://www.irishstatutebook.ie/eli/2005/act/14/enacted/en/html	Hard	Relevant to mention for two reasons. In the first place, while not a 'Data Protection Act', it nevertheless contained a strong form of data protection in Irish law with regard to genetics (testing and research). The relevant sections are part 4, section 42. Firstly, genetic testing should only be carried out on a person when that person's consent has been given to the processing of any genetic data derived from the testing. Secondly, the processing of genetic data is prohibited in relation to employment, insurance, health insurance, life assurance, occupational pension and the mortgaging of property. Thirdly, genetic data should not be processed unless all reasonable steps have been taken to provide the person with all appropriate information concerning the purpose and possible outcomes of the proposed processing, and any potential implications for the health of the person which may become known as a result of the processing. Importantly, this 2005 Disability Act (and its genetic data protection provisions) is also relevant because, unlike the repealed Data Protection Acts 1988/2003, it continues to have legal force alongside the 2018 Data Protection Act and GDPR itself. The Disability Act 2005 has been amended accordingly by the Data Protection Act 2018. http://www.irishstatutebook.ie/eli/2018/act/7/section/202/enacted/en/html
National Consent Policy	https://www.hse.ie/eng/about/who/qid/other-quality-improvement-programmes/consent/		National Health Service Executive (Ireland National Health Service) guidance for all staff regarding consent for all services users regarding all forms of interventions, interactions, research, etc.

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

(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?

Not at present.

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

Where processing takes place for law enforcement purposes (such as preventing or detecting crime) the GDPR does not apply, and instead the 'Law Enforcement Directive' covers these situations, the rules for which are found mainly in Part 5 of the Data Protection Act 2018 (which implements the Law Enforcement Directive into Irish law).

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 Data Protection Commission (DPC)	https://www.dataprotection.ie/	Yes	Approx. 110	Significant. The data protection authority that preceded the Data Protection Commission received complaints (e.g. relating to access rights, electronic direct marketing, unauthorized access, etc) in the following numbers (per year): 910 (in 2013) 960 (in 2014) 932 (in 2015) 1,479 (in 2016) 2642 (in 2017) 1249 (Jan to May 2018 – pre-GDPR) 2864 (May-Dec 2018 – post-GDPR) = noting that the highest absolute number is post-GDPR, while this	During the period 25 May — 31 December 2018, the DPC ran awareness-raising activities (under Article 57, GDPR). -- 260 complaints progressed to complaint-handling processes, including complaints transferred by other EU supervisory authorities, in respect of over 40 organisations. -- 15 statutory inquiries commenced.

				number is only for part of the year.	

Information regarding Data Protection Authority Ireland

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"?

Data processing for research purposes is not defined as such, but variously specified in The Data Protection Act 2018 (Revised 2019):

o Section 36(3c) 'research projects'

o Section 42 'processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'

Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018

- Research purposes is specified throughout as health-related

(iv) Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

- Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018

o Specifies provisions for where public interest in carrying out health research outweighs requirements for explicit consent (incl. role for REC), but does not define what the public interest would be (the parameters would be for health research – health research, itself, is defined as any of the following scientific research for the purpose of human health (wherein the aforementioned public interest would seem to be with regards to): (i) research with the goal of understanding normal and abnormal functioning, at molecular, cellular, organ system and whole body levels, (ii) research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury, (iii) research with the goal of improving the diagnosis and treatment (including the rehabilitation and palliation) of human disease and injury and of improving the health and quality of life of individuals, (iv) research with the goal of improving the efficiency and effectiveness of health professionals and the health care system; (v) research with the goal of improving the health of the population as a whole or any part of the population through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status.

- Data Protection Act 2018 (Revised 2019)

o Sections 42, 54, 55 & 61. all include provisions for the regulation, and sometimes restriction of data protection rights for individuals for archiving purposes in the public interest (and scientific or historical research purposes or statistical purposes) but without any specification or definition of what the public interest would be.

(v) 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?

Data Protection Act 2018 (Revised 2019)

Section 42 states that "subject to suitable safeguards for the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89, for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. This processing of personal data shall be subject to the principle of data minimisation and the adherence to processing without the identification of data subjects where possible.

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

Data Protection Act 2018 (Revised 2019)

Section 42 states that "subject to suitable safeguards for the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89, for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. This processing of personal data shall be subject to the principle of data minimisation and the adherence to processing without the identification of data subjects where possible.

(vii) 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.)?

- 'Policy statement on Ensuring Research Integrity in Ireland' (2019) Second Edition. Research Integrity National Forum

o The aim of the policy statement is to commit the main organisations in Irish research to the highest standards of integrity in carrying out their research so that partners, the public and other stakeholders, and the international research community have full confidence in the Irish research system. Primary responsibility for observing good practice in the use, storage, retention and preservation of data sits with the individual researcher, supported by the institution and in accordance with the guidelines in the policy statement. Specific points refer to the proper management and protection of data and research materials in all their forms (encompassing qualitative and quantitative data, protocols, processes, other research artefacts and associated metadata). Also highlighted is the necessity for researchers to constantly be aware of the provisions of, and operate in accordance with, Data Protection legislation which, amongst other things, sets out the conditions for usage of sensitive and personal data in health research. Research institutions and research funders are expected to remain abreast of current legislation pertinent to research and ensure that they and their staff act in accordance with legal and ethical provisions and codes relevant to their discipline at all times. Researchers are also expected to be aware that under Freedom of Information legislation, the researcher institution or organisation is required to allow persons access to documents of the institution (documents that are in the institution's possession) under defined circumstances. Researchers are to, at all times, be aware of the provisions of, and operate in accordance with, Data Protection legislation which, amongst other things, sets out the conditions for usage of sensitive and personal data in health research. In accordance with wider European codes, researchers are expected to have due regard for the health, safety and welfare of the community, of collaborators and others connected with their research, with research protocols taking sensitive to relevant differences in age, gender, culture, religion, ethnic origin and social class. Researchers are also expected to recognise and manage potential harms and risks relating to their research. The research is to be

conducted as confidentially as possible, in order to protect those involved in the investigation. Such confidentiality is to be maintained provided this does not compromise the investigation of the allegation, health and safety and the safety of participants in research. Where possible, any disclosure to third parties should be made on a confidential basis. If the organisation and/or its staff have legal obligations to inform third parties of research misconduct allegations, those obligations must be fulfilled at the appropriate time through the correct mechanisms. The policy document also outlines processes for addressing research misconduct.

https://www.iua.ie/wp-content/uploads/2019/08/IUA_Research_Integrity_in_Ireland_Report_2019.pdf

- The National Consent Policy (2019) Health Services Executive (HSE)

o The National Consent Policy provides one overarching HSE policy to guide staff regarding the need for consent, and the application of the general principles in this policy, which extends to all interventions conducted by or on behalf of the HSE in all locations. In terms of research participants, it is emphasised that they should be informed of the types of data required, the methods used to collect it and how the data will be utilised during the course of the study. Research participants are to be told how long their data will be retained and how it will be disposed of. They will also be given a description of any other aspects of the study, e.g. whether questionnaires or diary cards will be used. It is emphasised that it is important that consent be sought from research participants should there be secondary uses planned for the data e.g. future research studies. Participants are to be informed what information will be collected and for what purposes, in what form the data will be stored (e.g. de- identified) and what measures the researchers will put in place to ensure confidentiality for the full life-cycle of the study. In addition, research participants will be told which persons will have access to their data including third parties outside the jurisdiction, the risks of re-identification in event of data security breaches.

https://www.hse.ie/eng/about/who/qid/other-quality-improvement-programmes/consent/national-consent-policy-hse-v1-3-june-2019.pdf

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

Data Protection Act 2018 (Revised 2019)

Sections 42, 54, 55 & 61. all include provisions for the regulation, and sometimes restriction of data protection rights for individuals for collection and storage in the public interest (such as statistical purposes) but without any specification or definition of what the statistical purposes would be for. Rules applied under public interest above.

(ix) 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.)

- Data Protection Act 2018 (Revised 2019)

o Designation of data protection officer 34(1) Data Protection Act 2018

o The duty to collect consent is specified in section 55 where: "the data subject has given explicit consent to the processing for one or more specified purposes except where the law of the European Union or the law of the State prohibits such processing"

- Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018

o The duty to collect consent is specified in section 3(e) where it requires that: "explicit consent has been obtained from the data subject, prior to the commencement of the health research, for the processing of his or her personal data for the purpose of specified health research, either in relation to a particular area or more generally in that area or a related area of health research, or part thereof."

14.1.2 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)?

- Data Protection Act 2018 (Revised 2019)

o Section 33, "in accordance with Article 17, a controller shall, at the request of a data subject, without undue delay erase personal data of the data subject where the data have been collected in relation to the offer to that data subject of information society services referred to in Article 8(1)".

- 2005 Disability Act

o As noted above, there are additional levels of protection regarding consent and processing of data where genetics is concerned, under the ongoing 2005 Disability Act.

14.1.3 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)?

2005 Disability Act

As noted above, there are additional levels of protection regarding consent and processing of data where genetics is concerned, under the ongoing 2005 Disability Act.

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

Data Protection Act 2018 (Revised 2019)

The Data Protection Act 2018 gives further effect to the GDPR and has set the age of digital consent at 16, which means that if an organisation is relying on consent as the legal basis (justification) for processing a child's personal data and the child is under 16, then consent must be given or authorised by the person who has parental responsibility for the child.

Otherwise, for data protection purposes, a child is somebody under the age 18. Data protection rights apply to children just as much as they do to adults. However, there are child-specific protections attached to some of these provisions, which organisations must

take into account. For example, organisations have an express obligation under the GDPR to ensure that any transparency information about data processing which is addressed to a child should be in clear and plain language so that the child can understand it.

For instance, section 32. it encourages "the drawing up of codes of conduct intended to contribute to the proper application of the Data Protection Regulation with regard to: (a) the protection of children, (b) the information to be provided by a controller to children, (c) the manner in which the consent of the holders of parental responsibility over a child is to be obtained for the purposes of Article 8, (d) integrating the necessary safeguards into processing in order to protect the rights of children in an age-appropriate manner for the purpose of Article 25, and (e) the processing of the personal data of children for the purposes of direct marketing and creating personality and user profiles."

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

Not specified under the Data Protection Acts 2018, but is covered in the National Consent Policy (2019) Health Services Executive (HSE) and by Research Ethics Committees.

14.1.4 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?

The Irish Data Protection Acts do not apply to records of deceased persons.

14.1.5 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?

The Irish Data Protection Act (2018: Revised 2019) outlines procedure of accountability of the Commissioner for Data Protection to Oireachtas Committees (Irish Parliamentary Committees for, amongst other things, oversight).

14.2 Commercialization of data

14.2.1 General Regulatory Framework

No specific regulation discovered, also data commercialisation not mentioned in Data Protection Acts 2018 (Rev 2019) nor is it addressed in the 2018 annual report of the new (post-GDPR enactment) Data Protection Commission (DPC). While there is little sign of regulation and low levels of information, it is clear that data is being exchanged with private commercial entities on a regular basis (such as Facebook, Instagram).

This section is currently being investigated further before completion but it will more likely highlight that Ireland is currently unprepared in terms of legislation and regulation.

14.3 Security and cybersecurity

14.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Data Protection Act 2018 (Revised 2019)	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html http://revisedacts.lawreform.ie/eli/2018/act/7/revised/en/html (revised 2019)	Hard law	Provisions related to security are contained in the following sections: Section 41. The processing of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes (a) of preventing a threat to national security, defence or public security and (b) of preventing, detecting, investigating or prosecuting criminal offences -------- Section 55. Exemptions to measures for safeguarding the fundamental rights and freedoms of the data subject can be made in order to: (a) assess the risk of fraud or prevent fraud, (b) assess the risk of bribery or corruption, or both, or to prevent bribery or corruption, or both, or (c) ensure network and information systems security, and prevent attacks on and damage to computer and electronic communications systems. ----- 60(1) Such exemptions are also made: (i) to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State, (ii) for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, -

			60(7) Important objectives of general public interest above include: (a) preventing threats to public security and public safety; (b) avoiding obstructions to any official or legal inquiry, investigation or process, including any out-of-court redress procedure, proceedings pending or due before a court, tribunal of inquiry or commission of investigation; (c) preventing, detecting, investigating and prosecuting breaches of discipline by, or the unfitness or incompetence of, persons who are or were authorised by law to carry on a profession or any other regulated activity and the imposition of sanctions for same; (d) preventing, detecting, investigating or prosecuting breaches of ethics for regulated professions; (e) taking any action for the purposes of considering and investigating a complaint made to a regulatory body in respect of a person carrying out a profession or other regulated activity where the profession or activity is regulated by that body and the imposition of sanctions on foot of such a complaint; (f) preventing, detecting, investigating or prosecuting, whether in the State or elsewhere, breaches of the law which are subject to civil or administrative sanctions and enforcing such sanctions; (g) the identification of assets which are derived from, or are suspected to derive from, criminal conduct and the taking of appropriate action to deprive or deny persons of those assets or the benefits of those assets and any investigation or preparatory work in relation to any related proceedings; (h) ensuring the effective operation of the immigration system, the system for granting persons international protection in the State and the system for the acquisition by persons of Irish citizenship, including by preventing, detecting

			and investigating abuses of those systems or breaches of the law relating to those systems; (i) safeguarding the economic or financial interests of the European Union or the State, including on monetary, budgetary and taxation matters; (j) safeguarding monetary policy, the smooth operation of payment systems, the resolution of regulated financial service providers (within the meaning of the Central Bank Act 1942), the operation of deposit-guarantee schemes, the protection of consumers and the effective regulation of financial service providers; (k) protecting members of the public against— (i) financial loss or detriment due to the dishonesty, malpractice or other improper conduct of, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate or other entities, (ii) financial loss or detriment due to the conduct of individuals who have been adjudicated bankrupt, or (iii) financial loss or detriment due to the conduct of individuals who have been involved in the management of a body corporate which has been the subject of a receivership, examinership or liquidation protecting: (i) the health, safety, dignity, well-being of individuals at work against risks arising out of or in connection with their employment, and (ii) members of the public against discrimination or unfair treatment in the provision of goods or services to them
Criminal Justice (Offences Relating to Information Systems	http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/print.html	Hard	The Criminal Justice (Offences Relating to Information Systems) Act 2017 came into force on 12 June 2017, giving effect to Directive 2013/40/EU regarding criminal attacks against information systems. Such activities addressed by the 2017 Act: => Hacking covered by Section 2: A person who, without lawful authority or reasonable

) Act 2017			excuse, intentionally accesses an information system by infringing a security measure shall be guilty of an offence. => Denial of service attacks covered by Section 3: A person who, without lawful authority, intentionally hinders or interrupts the functioning of an information system by: (a) inputting data on the system, (b) transmitting, damaging, deleting, altering or suppressing, or causing the deterioration of, data on the system, or (c) rendering data on the system inaccessible, shall be guilty of an offence. => Infection of IT systems with malware (including ransomware, spyware, etc) is covered by Section 4: A person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of, data on an information system shall be guilty of an offence. => Possession or use of hardware/software to commit cybercrime covered by Section 6: A person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under section 2, 3, 4 or 5: (a) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or (b) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed, shall be guilty of an offence. => Identity theft or identity fraud is covered by Section 8.4.a: (4) (a) Where a court is determining the sentence to be imposed on a person for an offence under section 3 or 4 , the fact that the commission of the offence involved misusing the personal data of another person ("rightful identity owner") with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, shall be

			treated as an aggravating factor for the purpose of determining the sentence.

Main regulatory tools addressing security and cybersecurity in Ireland

14.3.2 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?

(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?

The Security of Network and Information Systems (NIS) Directive 2016/1148/EU was transposed into Irish law in September 2018 under the S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.

In addition, there is e-Privacy Regulations 2011 (S.I. 336 of 2011) implementing the e-Privacy Directive 2002/58/EC which regulates how public telecommunication networks manage personal data and requires those providers to undertake the appropriate technical and organisational measures to safeguard the security of its services and report incidents.

14.3.3 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 2018 requires data controllers to take appropriate measures, such as pressing charges for various cybercrimes (such as hacking, etc) with fines and/or custodial penalties. The Act does not specify particular security measures to be undertaken, but such decisions are guided by technical possibilities and costs. The Data Protection Commission issues guidance on introductions such as access controls, encryption, anti-virus software, firewalls, etc.

14.3.4 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?

The Data Protection Commission is the supervisory body overall. However, the Garda National Economic Crime Bureau (Garda = Irish police force) has broad authority to investigate cybersecurity (including searching of premises and seizing of equipment.

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

Tort cases can be taken and insurance can be taken out.

14.4 Enforcement: fines and sanctions

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

Criminal Justice (Offences Relating to Information Systems) Act 2017 - => Penalties are explicitly addressed in Section 8: depending on the particular act, a person who commits an offence may be liable to a class A fine (€5000+) or imprisonment for a term not exceeding 12 months, 5 years, or 10 years.

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

The Data Protection Commission can issue data controllers/processers an information notice (requiring information) or an enforcement notice (requiring certain action). If not complied with, it can impose administrative fines of €5000 max or imprisonment for 12 months max, or both, on summary conviction; or a fine of €250,000 max or imprisonment of 5 years max, or both. In terms of public bodies, the Data Protection Act 2018 provides for fines up to €1,000,000. The Act also allows for the Data Protection Commission to impose fines up to €20,000,000 in accordance with Article 83 of the GDPR.

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

They constitute an official offence.

14.5 Governance

(iv) 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?

(v) 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?

(vi) 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?

In health research/biomedical sciences, the (above noted) the appropriate governance structures for the carrying out of the research must include: ethical approval by a research ethics committee, assignment of relevant data controller and data processors involved, identification of funders and any other to who data may be shared to (incl. anonymised data) and provision of appropriate training must be provided. Other governance requirements on the management and conduct of the research include the performance of an initial assessment of the data protection implications of the health research and, where required under GDPR, a Data Protection Impact Assessment; in addition to implementing and testing security procedures.

Additionally, in terms of personal data breaches, the data processor must notify the data controller (i.e. the individual/legal entity who controls/responsible for collection/storage/use of personal information), who, in turn, must notify the Data Protection Commission with a description of the breach, likely consequences, planned remedial actions, etc. (unless the personal data breach is unlikely to result in a risk for the relevant individual's rights and freedoms).

Large companies and institutions also need to appoint a data protection officer (DPO)

A Privacy Impact Assessment to identify privacy risks is undertaken if personal data is used or being processed in research.

The Data Protection Commission is the overall data protection authority responsible for upholding the personal data protection rights specified by the GDPR.

Defence and security matters are generally covered in the Data Protection Act 1988/2018 - the Minister for Defence may – in relation to personal data kept by him in relation to the Defence Forces, designate an officer of the Permanent Defence Force who holds a commissioned rank therein to be a controller. [The DPA 2018 serves to repeal the Data Protection Acts 1988 to 2003, except for provisions relating to the processing of personal data for the purposes of national security, defence, and international relations of the State. The collective citation is now 'the Data Protection Acts 1988 to 2018'.]

15 Italy

Denise Amram; Giovanni Comandé (Scuola Superiore Sant'Anna)

15.1 Informed consent

15.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope