(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35 ; and

(f) any other information requested by the supervisory authority."

The above-mentioned process ensures the fulfilment of personal data processing requirements for research. So, all research process is monitored by **the State Data Protection Inspectorate**.

(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?

Such instruments are not known.

Data protection officers or the supervisory authority (The State Data Protection Inspectorate) usually advise on data protection issues. The Lithuanian Bioethics Committee shall analyse problems of bioethics and consult state and municipal institutions, agencies and organisations on the issues of bioethics

(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?

There is no national specific regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes. The Lithuanian Bioethics Committee shall issue approvals to conduct biomedical research and undertake ethical supervision of such research. In this case, it applies only to medical devices.

There are known cases when the authorities themselves set requirements for the processing of personal data in the context of scientific research. Such requirements are set out in a local document – the Policy.

Such tools are not known.

18 Luxembourg

Regina Becker (University of Luxembourg)

18.1 Informed consent

18.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law of 1 August 2018 on the organization of the National Commission for Data Protection and the General Scheme on Data Protection	http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo English translation by National Data Protection Authority: Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework	Hard law	Data protection law to implement the GDPR and to establish a supervisory authority. While it does cover research aspects, healthcare matters are being referred to sector law (not yet implemented)
Law of May 30, 2005, as amended, relating to specific provisions for the protection of the individual with regard to the processing of personal data in the electronic communications sector and amending Articles 88-2 and 88-4 of the Code criminal investigation.	http://legilux.public.lu/eli/etat/leg/memorial/2011/172#page=5&zoom=125,0,300		The law of May 30, 2005, amended by the law of July 27, 2007 , transposes into Luxembourg law the European Directive 2002/58 / EC . It regulates the protection of personal data in the field of telecommunications and electronic communications and takes into account recent and foreseeable developments in the field of electronic communications services and technologies. The 2005 law was further amended by the law of 24 July 2010, which is a transposition of Directive 2006/24 / EC of 15 March 2006. In addition, the law of 28 July 2011 transposes certain

			provisions of Directive 2009/136 / EC of 25 November 2009.

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

(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?

Law of 11 August 1982 concerning the protection of privacy.

http://legilux.public.lu/eli/etat/leg/loi/1982/08/11/n6/jo

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

Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal matters and on national security

http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a689/jo

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?
Commission Nationale pour la protection de la données (CNPD)	https://cnpd.public.lu/en.html	Yes	32	The data protection authority is organising regularly sessions to raise awareness and train people about the Data Protection European Regulation. In 2018 they trained more than 500 people in 12 sessions on "Data Protection Basics ".They also participate to conferences for more specialised audiences. They provided guidance and published guidelines about video surveillance, the right of personal portrayal (droit à l'image), data protection rules in the context of social elections and for associations; They also published forms to simplify the performance of their obligations by the controllers. However, with the advent of the GDPR, the availability for individual meetings has gone down considerably.

Information regarding Data Protection Authority Luxembourg

(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.?

No specific definition of what "data processing for research" includes was given nor is "research in the public interest" defined.

In practice, we follow the common approach (also recommended by the EDPB) that a public institution established by law with research in its mission pursues research in the public interest if it fulfils research as part of its defined portfolio.

(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?

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller of processing carried out for scientific or historical research purposes or statistical purposes, must implement the following additional appropriate measures:

1. the appointment of a data protection officer;

2. the performance of an impact assessment of the planned processing activities on the protection of personal data;

3. the anonymisation and pseudonymisation as defined in Article 4, paragraph 5 of Regulation (EU) 2016/679, or other operational separation measures guaranteeing that the data collected for scientific or historical research purposes or statistical purposes, cannot be used to adopt decisions or take actions concerning data subjects;

4. the use of a trusted third party, operationally independent from the controller, for the anonymisation or pseudonymisation of the data;

5. the encryption of personal data in transit and at rest, as well as state of the art key management;

6. the use of technology reinforcing the protection of the private lives of data subjects;

7. the use of access restrictions to personal data within the controller;

8. the use of a log file enabling the reason, date and time that data is consulted and the identity of the person collecting, modifying or deleting personal data to be retraced;

9. promoting the awareness of the staff involved about the processing of personal data and professional secrecy;

10. the regular evaluation of the effectiveness of the technical and organisational measures implemented through an independent audit;

11. the prior drawing up of a data management plan;

12. the adoption of the sector specific codes of conduct as set out in Article 40 of Regulation (EU) 2016/679, approved by the European Commission pursuant to Article 40, paragraph 9 of Regulation (EU) 2016/679.

For each project for scientific or historical research purposes or statistical purposes, the controller must document and justify any exclusion of one or several of the measures listed in this article.

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

No sensitive data are defined beyond the special categories of the GDPR.

The implementation of 9(2)j was done in the law of 1 August 2018 through Art. 64 :"The processing of special categories of personal data as defined in Article 9, paragraph 1 of Regulation (EU) 2016/679, may be carried out for the purposes referred to in Article 9 paragraph 2, point j) of this same regulation, if the controller meets the requirements set out in Article 65."

Furthermore, the following restriction is defined in Art. 66:

The processing of genetic data for the purposes of the exercise of the specific rights of the controller in the field of labour law and insurance is prohibited.

(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 is currently no Code of Conduct for data processing in research in place yet, but there is an initiative led by ELIXIR-LU together with the public research stakeholders to develop a Code of Conduct for Scientific Research.

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

No, there is no special definition for statistical purposes given. No special rules apply, they are the same rules as defined for scientific research (see above).

(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.)

The above-mentioned law of 1 August 2018 covers the processing of data for research purposes including required safeguards.

In addition, the national data protection authority has published a DPIA Black List that requires a DPIA for processing under Art. 63-65. Due to the generic phrasing of Art. 65, our conclusion is that any scientific research will require a DPIA. As this is not compatible with the idea of a DPIA, the National GDPR Working Group for Research is raising this subject with the CNPD.

Archiving law (Law of 17 August 2019), referring to the transfer of data from public archives for research and scientific activities if these are in the public interest and do not impact overly the privacy of the affected data subjects.

18.1.2 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.)

Article 63 of the Law of 1 August 2018 allows the derogation of data subjects' rights under Articles 15, 16, 18 and 21 GDPR provided the safeguards of Art. 65 are applied.

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

No.

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

No.

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

No; nothing other than the derogation as above.

18.1.3 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)?

No there not

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

No. A minor can give consent from the age of 16.

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

The applicable law do not contain special provisions for other potentially vulnerable groups.

18.1.4 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?

No special provisions about the processing of data of deceased persons exit in Luxembourg.

18.1.5 Accountability and Data Protection Impact Assessment

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

In case of processing personal data for research, a controller has to justify and document why safeguards as listed in the law of 1 August 2018 are not implemented

(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?

A guidance on DPIAs was published on the webpage of the supervisory authority including a template to ask for a consultation: https://cnpd.public.lu/en/professionnels/obligations/AIPD.html

Please note that the French webpage is usually more complete and includes also the DPIA Black List: https://cnpd.public.lu/fr/professionnels/obligations/AIPD.html

This Black List published by CNPD requires a DPIA for all cases of processing special categories of data for research without consent, for a derogation of data subjects' rights in the context of processing for scientific research and – by accident – they seem to require a DPIA for all research processing of personal data. This is currently subject to a discussion on the national level.

18.2 Commercialization of data

18.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Loi du 18 avril 2004 modifiant 1) la loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données, et 2) la loi modifiée du 20 juillet 1992 portant modification du régime des brevets d'invention **(April 18, 2004 of the Act to Amend - 1. Law of 18 April 2001 on copyright, related rights and databases, and 2. the amended law of 20 July 1992 amending the rules on patents)**	http://legilux.public.lu/eli/etat/leg/loi/2004/04/18/n4/jo With automatic translation tool: https://wipolex.wipo.int/en/text/128654	Hard law	Relative law that amends the existing laws on copyright and patents
Loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données **(Act of 18 April 2001 on copyright, related rights and databases)**	http://legilux.public.lu/eli/etat/leg/loi/2001/04/18/n2/jo With automatic translation tool: https://wipolex.wipo.int/en/text/128652	Hard law	Covering the sui generis right on databases

Main regulatory tools addressing data commercialization in Luxembourg

18.2.2 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)?

Yes.

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

No specific information.

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

No.

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

Some sectorial laws mentioned the possible use of personal data in the public sector for research purposes (e.g. social data). There is also a law for public sector data. This law excludes protected data as well as data located in research institutions.

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

No, nothing beyond copyright law.

18.2.3 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?

No special classification exists in Luxembourg laws.

(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?

Protection of databases and copyright are covered by the same law (see table above).

18.3 Security and cybersecurity

18.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of security of networks and information systems in the Union European Parliament	http://data.legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo	Hard law	Implementation of NIS Directive

Main regulatory tools addressing security and cybersecurity in Luxembourg

18.3.2 Implementation of EU Law

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

Security requirements provided by law for Operators of Essential Services and Digital Service Providers are largely based on the requirements set by the NIS Directive:

- Take technical and organisational measures to manage the risks posed to the security of networks and information systems [Art. 8 (1), Art. 11 (1)].

- Provide to NCAs information needed to assess the security of networks and information systems, including security policies [Art. 9 (1) para 1, Art. 12 (1) para 1].

- Provide to NCAs evidence of effective implementation of security policies, such as the results of security audits [Art. 8 (1) para 2].

- Provide to NCAs any information needed to control the effective implementation of security policies [Art. 8 (1) para 3, Art. 11 (1) para 3].

- Remedy any failure to meet the security requirements [Follow the binding instructions to remedy deficiencies identified [Art. 9 (2)]].

- Remedy any failure to meet the security requirements [Art. 11 (1) para 2].

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

The NIS Directive was implemented through the law of 28 May 2019 (see link above).

(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?

No regulation beyond the above-mentioned measures.

18.3.3 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?

No requirements for data breach notification in general have been implemented in Luxembourgish law. The national implementation of the NIS Directive regulates data breach notifications (incident notifications) for IT services.

Operators of Essential Services (OES) shall notify any incident having a “significant” impact while Digital Service Providers (DSPs) shall notify any incident having a “substantial” impact without undue delay as referred in Art. 8 (4) and 11 (3) of the law of 28 May 2019. The law, however, does not clarify the undue delay.

Criteria to determine substantial impact:

- Number of users affected by incident
- Duration of the incident
- Geographical spread with regard to area affected by incident
- Extent of disruption of the functioning of the service
- The extent of impact on economic and societal activities

Criteria to determine significant impact:

- Number of users affected by incident
- Duration of the incident
- Geographical spread with regard to area affected by incident

OES shall notify Institute of Regulation (ILR) or the Financial Sector Supervisory Commission (CSSF) (the notification shall subsequently be transmitted to CERT Gouvernemental (GovCERT) or the Computer Incident Response Centre Luxembourg (CIRCL)), while DSPs directly notify GovCERT and/or CIRCL. In accordance with the commentary of Art. 10 of the law of 28 May 2019, neither ILR nor CSSF have the authority to supervise the activities of DSPs. Therefore, incident notification requirements will automatically apply to all DSPs, without prior obligation to contact the National Competent Authorities.

Under Article 10 of the law, it is foreseen to introduce a unified incident notification platform in order to notify incidents directly to the Computer Security Incident Response Teams. An example of a widely-used platform for incident notification and exchange in support of the NIS Directive is the Malware Information Sharing and Threat Intelligence Sharing Platform (MISP).

18.3.4 Supervision of cybersecurity

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

Art. 3 of the law of 28 May 2019 establishes the National Competent Authorities (NCAs) as foreseen in the NIS Directive in Luxembourg. These are the Institute of Regulation (ILR) and the Financial Sector Supervisory Commission (CSSF). The ILR will be considered to be the NCA for the energy, transport, drinking water supply and distribution sectors as well as the health sector. According to the Art. 4 of the draft law it will also be a single point of contact (SPOC) that will coordinate NIS related activities and ensure cross border cooperation.

Since the CSSF is already regulating the financial sector in Luxembourg, within Art. 4 of the draft law states, it will be considered as the NCA for the banking and financial market infrastructure sectors.

(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 role of the German BSI is not clear to me. Therefore, a comparison is difficult. See bodies mentioned above.

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

To my knowledge, there is no regulation by law on claims after lack of cybersecurity. The damaged party has to sue the offender.

18.4 Enforcement: fines and sanctions

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

Law of 18 July 2014 on cybercrime stipulates penalties of four months to five years imprisonment and a fine of 1,250 euros to 30,000 euros.

Law of 11 August 1982 concerning the protection of privacy: Imprisonment and fines for violation of privacy as defined in Art. 2 of the law (e.g. interception of letters).

Law of 1 August 2018: Any person who wilfully prevents or impedes, in any way, the execution of the tasks of the CNPD, shall be sentenced to imprisonment for a period of eight days to one year and a fine of 251 to 125 000 euros or one of these punishments alone.

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

Yes.

In the law of 1. August 2018 fines can be issued:

- In cases as foreseen in Art. 83 GDPR (except against the State or municipalities).
- In cases of a violation of Article 10 GDPR (except against the State or municipalities)

In the law of 28 May 2019 in case of failure to comply with the obligations fines can be issued of which the amount can go up to 125,000 EUR.

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

They constitute an official offence.

18.5 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?

Data protection aspects are covered by the Institutional Review Boards (IRBs) of individual research institutions. All projects dealing with personal data should be submitted to the IRB based on an application form. Approval has to be obtained before the research commences. However, there is no enforcement. Also, there is no monitoring of the research process

(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?

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