provide information would need a disproportionate effort or compromise the aims of the research. In these cases, specific organizational and technical measures to ensure fundamental rights should be implemented, the approval of the ethical committee is needed and a prior consultation under article 36 is performed.

The Ethics rules on data processing for scientific research or statistical purposes refers to biomedical science establishing as follows. For medical, biomedical, epidemiological research, article 8 of the above-mentioned ethics rules states that data subjects/patients should be able to distinguish through proper information between data flows for healthcare purposes and data flows for research purposes, but consent seems to be maintained as the principal legal basis to process data. This might be misled if it is not compared with article 110 of the Data Protection Act Legislative Decree n. 196/2003, as amended by the Legislative Decree 101/2018, a higher ranking rule. It states, in fact, that consent it is not necessary if the legal basis is article 9, para 2, sub j) and a data protection impact assessment has been performed and published. The provision is quite cryptic as it is not evident which are the cases where article 9, para 2, sub j) is not applicable and it does not explain how the data protection impact assessment should be published to fulfil the requirements. Furthermore, according to the mentioned article, the consent is not required whether there is a positive approval from an ethical committee and a prior consultation before the data protection authority has been performed. Also this exception may create some practical issues if we consider that data protection is an ethical profile that an ethical committee should face in its opinion. The relationship between data protection compliance and ethical compliance is, again, recalled within the article 8 of the ethics rules. Its para 4, indeed, states that the informed consent under the Oviedo Convention and Helsinki Declaration shall include information about incidental findings, while in the previous paragraphs the topic was the legal basis for data processing. This combination of provisions on privacy information and informed consent misleads the GDPR paradigm which promotes data circulation, under the principles of data protection by design and by default, instead of requiring the data subject's consent.

These profiles should be evaluated at the ethical committees' level. However, it's not mandatory to include an expert of data protection within the ethical committees.

16 Latvia

Liene Labsvīra (Legal Adviser of the European Union, International Cooperation Division of the State Data Inspectorate)

16.1 Informed consent

16.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation	Brief description and scope
Personal Data	https://likumi.lv/ta/en/en/id/300099-	Hard law	GDPR implementation law

Processing Law	personal-data-processing-law		
Aircraft Passenger Data Processing Law	https://likumi.lv/ta/en/en/id/288544-aircraft-passenger-data-processing-law	Hard law	National law regulating processing of passenger's' data with aim to prevent and detect potential terrorism, national security treats and serious crime.
Biometric Data Processing System Law	https://likumi.lv/ta/en/en/id/193111-biometric-data-processing-system-law	Hard law	National provisions relating to establishing and maintenance of state data base of biometric data of natural persons' biometric data
Human Genome Research Law	https://likumi.lv/ta/en/en/id/64093-human-genome-research-law	Hard law	Provides genetic research regulations in relation to the genome database and organisation of the supervision of such research.
Law regarding personal data processing in criminal proceedings and procedure of administrative offenses	https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa	Hard law	Regarding personal data processing of authorities with aim and during for the detection, investigation, and prosecution of criminal offences
Law On the Rights of Patients	https://likumi.lv/ta/en/en/id/203008-law-on-the-rights-of-patients	Hard law	Regulates some aspects of informed consent.
Law On Information Society Services	https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services	Hard law	Law provides procedure of provision of information society services

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

(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?

National law does not provide any additional protection of personal data used purely for personal or household activity in so far as it can be assumed as personal or household activity.

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

National regulatory framework empowers the National Security Authorities collect, accumulate, analyse political, economic, social, military, scientific, technical and other information with aim to detect potential internal or external threat to the independence of state, constitutional order and territorial integrity. It is not directly stated that these powers include personal data processing but it is apparent from the substance of this system.

National law "Personal Data Processing Law" provides restriction of data subject's rights of access in favour of interests of national security or national safety (Art.27(1))

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Datu valsts inspekcija (Data State Inspectorate)	https://www.dvi.gov.lv/lv/ https://www.dvi.gov.lv/en/	Yes	25 Staff positions + 1 temporary position	5 points of 10	Within 30 days generally

Information regarding Data Protection Authority

(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.?

National law "Personal Data Processing Law" foresees personal data processing for Scientific or Historical Research Purposes (Art.31).

There are specific fields of research covered by national law such as genetic research, medical research and research of documents of former Committee for State Security (KGB) of the Latvian Soviet Socialist Republic.

(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?

This mechanism is partly covered in national legislation, in field of medical research and human genome research.

For example national law "Law On the Rights of Patients" (English version available here: https://likumi.lv/ta/en/en/id/203008-law-on-the-rights-of-patients) provides some mechanisms of safeguards (see Art.10(7) and Art.11)

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

Please see answer to the previous question

(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 codes of conduct for data processing in Latvia yet.

In field of scientific research there is Code of Ethics for Scientists available (approved in Meeting of the Latvian Academy of Sciences) that covers some aspects of data processing.

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

In field of scientific research there is Code of Ethics for Scientists available (approved in Meeting of the Latvian Academy of Sciences) that covers some aspects of data processing.

(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.)

These mechanisms are partly covered in national legislation, in field of medical research and human genome research but duties to appoint DPO, DPIA and others are covered by GDPR.

16.1.2 Rights of data subjects and data processing

(i) Are there any particularities regarding data subjects at the national level?

Part of national normative acts specifies situations when data subject's rights may be restricted.

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

Construct of informed consent is present in field of medicine that includes personal data including special categories of data (health data, genetic data) processing

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

GDPR is considered as general regulatory framework in field of data processing and all normative acts at national level are being harmonized with requirements of GDPR in field of personal data processing.

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

-According to national normative acts data subject's rights may be restricted in specific circumstances.

16.1.3 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)?

GDPR is considered as general regulatory framework in field of data processing and all normative acts at national level should be harmonized with requirements of GDPR in field of personal data processing.

GDPR and normative acts at national level in field of personal data processing do not cover information concerning legal persons, except, data of natural persons in cases if exception laid down in Recital 14 of the Preamble of GDPR is not applicable.

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

National law foresees that in 13 of age person is able to give consent for his or her personal data processing to provide information society services.

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

Generally, national regulatory framework recognizes other vulnerable person groups such as families with three or more children, one-parent families, people with disabilities, persons over working age, 15-25 age group, persons released from prisons and others depending of relevant normative act of national level. However, in field of personal data protection there are not listed other vulnerable person groups.

16.1.4 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?

Generally, national legislation does not cover personal data protection of deceased persons. However, it is prohibited disclose patient's data after person's death except to spouse or to the closest relative of the patient in case the criteria set in Law has been met (see Art.10(3), (4) of Law on the Rights of Patients).

16.1.5 Accountability and Data Protection Impact Assessment

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

National law does not foresee particular procedure for DPIA. However there are same guidelines in place issued by national data protection authority

(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?

Please, see the answer to the previous question

16.2 Commercialization of data

16.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law On Information Society Services	https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services	Hard law	Law provides procedure of provision of information society services
Freedom of Information Law	https://likumi.lv/ta/en/en/id/50601-freedom-of-information-law	Hard law	Law governs public access to documentation held by the public institution. Covers rights of natural or legal persons obtain information held by public entity.
Law on Submissions	https://likumi.lv/ta/en/en/id/164501-law-on-submissions	Hard law	Law establishes procedure for submission applications to public institutions by natural or legal person and obligations of institutions to provide the answer to the applicant
Administrative Procedure Law	https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law	Hard law	Law generally determines regime of administrative procedure in public institutions.
Procedure for granting exclusive rights for re-use of information and publishing information regarding granting of such rights	https://likumi.lv/ta/id/158245-kartiba-kada-tiek-pieskirtas-ekskluzivas-tiesibas-informacijas-atkalizmantosanai-un-publiskota-informacija-par-sadu-tiesibu-pie... (not available in English)	Cabinet Regulation (Hard law)	Normative act determines procedure for granting exclusive rights for providing information society services in the public interest
Regulations regarding Paid Services for the Provision of Information	https://likumi.lv/ta/en/en/id/148617-regulations-regarding-paid-services-for-the-	Cabinet Regulation (Hard law)	Normative act provides arrangements for payment for public information society services

	provision-of-information		
Procedure for posting information on the Internet by institutions	https://likumi.lv/ta/id/301865-kartiba-kada-iestades-ievieto-informaciju-interneta (not available in English)	Cabinet Regulation (Hard law)	Normative act f
Procedures for Protecting the Information for Official Use Only	https://likumi.lv/ta/en/en/id/107093-procedures-for-protecting-the-information-for-official-use-only	Cabinet Regulation (Hard law)	Normative act prescribes the procedures for protecting the information for official use only.

Main regulatory tools addressing data commercialization in Latvia.

1.4.1.1 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)?

National normative acts do not foresee such restriction in case all requirements applicable to such processing have been taken into account.

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

Requested information has not been collected or is not publicly available

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

National regulatory framework does not foresee any remuneration of data subjects.

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

Please, see table above

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

National regulatory framework does not foresee any specific protection for metadata or non-personal data. General national regulation relating to retention of the information and data is provided in national law "Archives Law"(English version (outdated only) available here: https://likumi.lv/ta/en/en/id/205971-archives-law *)*

16.2.2 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 special data classification foreseen in Latvia. In practice construct for data may depend on its use in particular circumstances. Data could be considered as product or commodity or good depending on particular situation.

(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?

National regulation protects such fields notion of data that value of data determine according to normative acts, legal doctrine, legal practice, case-law.

16.3 Security and cybersecurity

16.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law on the Security of Information Technologies	https://likumi.lv/ta/en/en/id/220962-law-on-the-security-of-information-technologies	Hard law	Main law at national level that regulates cyber security issues in Latvia
Aircraft Passenger Data Processing Law	https://likumi.lv/ta/en/en/id/288544-aircraft-passenger-data-processing-law	Hard law	National law regulating processing of passenger's' data with aim to prevent and detect potential terrorism, national security treats and serious crime.
Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements	https://likumi.lv/ta/en/en/id/275671-procedures-for-the-ensuring-conformity-of-information-and-communication-technologies-systems-to-minimum-security-requirements	Cabinet Regulation (Hard law)	Prescribes minimum of requirements for the information and communication technologies of the State and local government institutions
Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies	https://likumi.lv/ta/en/en/id/225776-procedures-for-the-planning-and-implementation-of-security-measures-for-the-critical-infrastructure-of-information-technologies	Cabinet Regulation (Hard law)	Prescribes the procedures for the planning and implementation of security measures for the critical infrastructure

Regulations Regarding the Information to be Included in the Action Plan of a Merchant of Electronic Communications, the Control of the Implementation of Such Plan and the Procedures, by which End Users shall be Temporarily Disconnected from the Electronic Communications Network	https://likumi.lv/ta/en/en/id/229559-regulations-regarding-the-information-to-be-included-in-the-action-plan-of-a-merchant-of-electronic-communications-the-control-of-the-implementation-of-such-plan-and-the-procedures-by-which-end-users-shall-be-temporarily-disconnected-from-the-electronic-communications-network	Cabinet Regulation (Hard law)	Prescribes what information must be included into action plan to ensure continuous operation of communication network, procedures for temporarily disconnection of end-users from network and criteria of significance of ICT security incidents
Electronic Communications Law	https://likumi.lv/ta/en/en/id/96611-electronic-communications-law	Hard law	Law governs competence, rights and duties of users, electronic communications service providers, private electronic communications network owners and State administrative institutions, which are associated with the regulation of the electronic communications sector, the provision of electronic communications networks and the provision of electronic communications services, as well as the use and administration of scarce resources.
Law On State Information Systems	https://likumi.lv/ta/en/en/id/62324-law-on-state-information-systems	Hard law	
National Security Concept	https://likumi.lv/ta/id/309647-par-nacionalas-drosibas-koncepcijas-apstiprinasanu	Policy planning document	Detects potential treats to national security, sets general priorities to prevent these treats, including cyber threats.

Cyber Security Strategy of Latvia	http://www.mrcc.lv/~/media/AM/Ministrija/Sabiedribas_lidzdaliba/2018/11/AIMstrat_kiber_projekts_181022.ashx (Latvian version only)	Policy planning document	Describes cyber security context of Latvia, identifies future challenges and national cyber security policy priorities
Information system security testing guidelines	www.varam.gov.lv/in_site/tools/download.php?file=files/text/publikacijas/metod/eparv//ISdrosParbVadl.pdf (Latvian version only)	Soft law	Guidance that describes minimum of requirements for safety of information systems of public sector.
Information Systems Security Management Implementation Guidelines	varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//VISvadlinijas.pdf (Latvian version only)	Soft law	Guidance to help organizations to implement appropriate internal policies.

Main regulatory tools addressing security and cybersecurity in Latvia

16.3.2 Implementation of EU Law

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

NIS Directive is transposed into a national law. Last amendments to national regulation came in to force on 15 January 2019 which relate to operators of essential services and digital service providers as well as owners and lessees of the ICT critical infrastructure and lay down minimum requirements for the safety that must be ensured to their ICT systems

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

Please see answer to previous question.

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

National regulation is being harmonized with GDPR requirements.

16.3.3 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?

Procedure for notification of data breaches differs from procedure for notification of information technology security incidents.

In case of data breach Controller is obliged to notify Data State Inspectorate according to procedure described by Data State Inspectorate (procedure available here (Latvia version only): https://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/). Obligation is based on GDPR.

In case of information technology security incident that has significant impact on the continuity of essential services (concerns essential services) and that has significant impact on the provision of the service (concerns digital services) operator of essential services and digital service provider are obliged to notify Information technology security incident prevention body, in Latvia – Cert.lv. Obligation is based on NIS directive.

16.3.4 Supervision of cybersecurity

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

In the Republic of Latvia exists several institutions with enforcement powers.

(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?

One institution similar to German BSI is not established in the Republic of Latvia. Functions related to cyber security are divided to several institutions.

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

There are several procedures to claim damages depending on current circumstances.

For example, in criminal proceedings victim may submit application for compensation. In case the State is responsible for such damages because of lack appropriate security or measures etc., the victim may claim damages against the State.

16.4 Enforcement: fines and sanctions

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

It is foreseen in national law "The Criminal Law" criminal liability for committing criminal offences related to data protection or cyber security.

The punishment for such types of crime can be imprisonment, short term of imprisonment, community work or fine which depends on committed type of the crime and other criteria

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

For illegal operations with personal data, failure to provide information to data subject or Data State Inspectorate may be imposed fine according to Latvian Administrative Violations Code despite the corrective measures set in GDPR.

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

Data protection offences constitute the official offence based on information about potential violation of law.

16.5 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?

In the Republic of Latvia, the Data State Inspectorate is the only body with powers to run the case related to personal data protection issues.

(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?

Requested information is not available.

(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?

This field is regulated by national regulation. Ministry of Defence and instructions authority of Ministry such as Latvian State Security Service are responsible monitoring and enforcement in this field. Detailed information is not available.

17 Lithuania

Danguolė Morkūnienė (State Data Protection Inspectorate)

17.1 Informed consent

17.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope