technologies can use in order to protect against industrial espionage and other confidentiality breaches?

The EU Dual-Use Regulation (EC) 428/2009 applies to research projects with export of technology or knowledge, unless the technology/knowledge is in the public domain. The Danish Business Authority is responsible for monitoring compliance with the Dual-Use Regulation and for granting export licenses when required by the Dual-Use Regulation.

Export of dual-use technology is not independently regulated by Danish national law. There are no additional requirements besides those that follow from the EU Dual-Use Regulation.

Finally, the Centre for Cyber Security are monitoring the area and has previously published a report describing the cyber risks related to research – e.g. the risks of espionage. As a result, the centre recommended that the individual research institutions take precautions and take initiatives that can prevent espionage, cyber-attacks etc.

8 Estonia

Lethe Roots (Aldon Konsultatsioonid OÜ)

8.1 Informed consent

8.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Regulation (EU) No 2016/679 (GDPR)	Regulation (EU) No 2016/679	Hard law	This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
Personal Data Protection Act (PDPA)	Personal Data Protection Act	Hard law	1. Protection of natural persons upon processing of personal data to the extent in which it elaborates and supplements the provisions contained in Regulation (EU) 2016/679; 2. Protection of natural persons upon processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments; 3. Supervision and formation of independent supervisory authority

			(Estonian Data Protection Inspectorate); 4. Liability for the violation of the requirements for processing of personal data. This Act provides for: i) standards for implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council; and ii) standards for transposition of Directive (EU) 2016/680 of the European Parliament and of the Council.
Public Information Act (PIA)	Public Information Act	Hard law	To ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties.
Electronic Communications Act (ECA)	Electronic Communications Act	Hard law	To ensure protection of personal data and confidentiality of all information which becomes known thereto in the process of provision of communications services, including: 1. information concerning specific details related to the use of communications services; 2. the content and format of messages transmitted over the communications network; 3. information concerning the time and manner of transmission of messages.
Archives Act (AA)	Archives Act	Hard law	This Act provides for the appraisal of records, acquisition and preservation of archival records, grant of access thereto, organisation of use thereof, and liability for rendering records and archival records unusable and destruction thereof, establishment of the bases for records management of agencies and persons performing public duties and the bases for the

			activities of the National Archives and local government archives.
State Secrets and Classified Information of Foreign States Act (SSCIFSA)	State Secrets and Classified Information of Foreign States Act	Hard law	The purpose of this act is to ensure the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure and becoming accessible to persons who have not been granted access to such information.
Security Authorities Act (SAA)	Security Authorities Act	Hard law	This Act provides for: 1. the functions and competence of security authorities in ensuring national security and constitutional order, and the procedure for the exercise of supervision over the activities of security authorities. 2. the processing of personal data, including special categories of personal data, and the restriction of the scope of the rights of data subjects by security authorities and the procedure for the exercise of supervision over compliance with the requirements for personal data processing.
Population Register Act (PRA)	Population Register Act	Hard Law	This Act provides for the composition of data in the population register and the procedure for the maintenance of the population register, entry of data on residence in the population register, provision of personal identification code, processing of data, ensuring access to data and exercise of supervision over such activities.
The Constitution of the Republic of Estonia **(Constitution)**	The Constitution of the Republic of Estonia	Hard law	Constitutional protection for: 1. person's private and family life; 2. right to confidentiality of messages sent or received by person by post, telegraph, telephone or other commonly used means;

			3. right to free self-realisation; 4. right to free access to information disseminated for public use.
General guidelines for processors of personal data	https://www.aki.ee/en/guidelines	Guidelines by Estonian Data Protection Inspectorate	Estonian Data Protection Inspectorate has published several guidelines for helping processors of personal data to implement regulations in regards personal data protection. Please note that there are presented greater number of guidelines in Estonian than in English.

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

(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?

These data categories are protected by the constitutional rights stated (especially in Article 26 of the Constitution, which states that everyone is entitled to inviolability of his or her private and family life) in the Constitution of the Republic of Estonia.

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

Yes, SAA covers the topic. The SAA provides for the bases for the processing of personal data, including special categories of personal data, and the restriction of the scope of the rights of data subjects by security authorities and the procedure for the exercise of supervision over compliance with the requirements for personal data processing.

Article 3 of SAA states that Security authorities (i.e. the Estonian Internal Security Service and the Estonian Foreign Intelligence Service as stated in Article 5 of SAA) are authorized to collect and process information, including personal data, insofar as this is necessary for performing its functions, considering the following principles:

1. the manner and scope of collection and processing of information and the organisational and technical safeguards applied may not excessively adversely affect the fundamental rights of a person compared to the objective pursued by the security authority;

2. the collection and processing of information may not endanger the life or health of a person, unnecessarily endanger property or the environment or unnecessarily infringe other personal rights;

3. information is processed and retained for as long as necessary for the performance of the security authority's function and in accordance with the objective of the activity of the security authority;

4. information is collected and processed in a manner which ensures its security, including protects against unauthorised or unlawful processing and accidental loss or

destruction thereof or damage thereto by applying appropriate technical or organisational measures.

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Estonian Data Protection Inspectorate	https://www.aki.ee/en	Yes	Approx. 20	Moderate	Moderate

Information regarding Data Protection Authorities, Estonia

(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.?

1. No, PDPA does not introduce a specific definition of "data processing for research purposes". Nevertheless Article 5 of PDPA states rules for processing of personal data for academic, artistic and literary expression, i.e. personal data may be processed without the consent of the data subject for the purpose of academic, artistic and literary expression, in particular disclosed if this does not cause excessive damage to the rights of the data subject.

Article 6 of PDPA states the rules for processing of personal data for needs of scientific and historical research and official statistics, i.e. personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic (for further details, please see the answer for the next question in regards implementation of Article 89 of GDPR.

2. No, PDPA does not define "research in public interest". Nevertheless Article 7 of PDPA is stating rules for processing of personal data for archiving in public interest and they are following:

2.1. If personal data are processed for the purpose of archiving in the public interest, the controller or processor may restrict the rights of the data subject provided for in Articles 15, 16 and 18-21 of GDPR insofar as the exercise of these rights is likely to make the achievement of the purpose of archiving in the public interest impossible or impedes it to a significant extent.

2.2. The rights of data subjects specified in section 2.1 may be restricted in order not to endanger the condition, authenticity, reliability, integrity and usability of the records.

(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?

Yes, national legislation has implemented Article 89 of the GDPR. Article 6 of PDPA regulates data processing for research purposes, including specific safeguards.

Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provides equivalent level of protection. Prior to transmission of personal data for processing for the needs of scientific and historical research or official statistics, personal data shall be replaced by pseudonymised data or data in a format which provides equivalent level of data protection.

Depseudonymisation or any other method by which the data not enabling identification of persons are changed again into the data which enable identification of persons are only permitted for the needs of additional scientific and historical research or official statistics. Processors of personal data shall designate a person identified by name who has access to the information allowing pseudonymisation.

Processing of data concerning any data subjects for the needs of scientific and historical research or official statistics without the consent of the data subject in a format which enables identification of the data subject is permitted only in the case the following conditions are met:

1. the purposes of data processing can no longer be achieved after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes;

2. there is overriding public interest for it in the estimation of the persons conducting scientific and historical research or compiling official statistics;

3. the scope of obligations of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner.

Article 6(4) of PDPA states that if scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.

Please note, Article 6(5) of PDPA states that scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development. In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided for in this section, except in the case the objectives of the studies conducted for policy development and the scope of processing of personal data derive from legislation.

Where personal data are processed for the purpose of scientific and historical research or official statistics, the controller or processor may restrict the rights of data subjects provided for in Articles 15, 16, 18 and 21 of GDPR insofar as the exercise of these rights is likely to make the achievement of the objectives of the scientific and historical research or official statistics impossible or impedes it to a significant extent.

(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, national legislation does not provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR.

(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.)?

Protection Inspectorate released a guideline in 2015 to regulate scientific researches what is based on special categories of personal data. Currently, Estonian Data Protection Inspectorate has stated on its website that the guideline is under review. Therefore, the (outdated) guideline will not be summarized here, because it is unknown on what scale the Estonian Data Protection Inspectorate shall amend this guideline or shall declare an entirely new guideline.

Article 6 (4) of PDPA states that if scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.

Therefore, ethics committee of the relevant area shall verify compliance of the planned research. For example, Research Ethics Committee of the University of Tartu (Committee) shall verify the compliance in accordance with its Statute, which states that the Committee shall:

1. assess the ethical aspects of human research in the field of medicine and natural science (incl. human gene research and clinical trials of medicinal products) and other human research, if danger to the physical or mental health of human(s) may occur with conducting the aforementioned research; and

2. follow in its activities the Constitution of the Republic of Estonia, the European Council's Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Additional Protocol to the Convention Concerning Biomedical Research, the Declaration of Helsinki of the World Medical Association, other generally recognized ethical rules and international conventions, the Medicinal Products Act, the Human Genes Research Act, the Personal Data Protection Act, and other relevant legislation as well as the good practice of conducting clinical trials.

(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, PDPA does not give a specific definition for "statistical purposes". To such data processing apply rules stated in Article 6 of PDPA (for further details, please see answer to the question "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?")

(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.)

No, there are not any other references. General requirements to have a DPO, to perform a DPIA, to collect consent, are stated in PDPA.

8.1.2 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.)

Yes, Article 18 of PDPA states that in processing of personal data by law enforcement authorities in prevention, detection and proceedings of offences and execution of punishments, if possible and appropriate, the controller shall distinguish, upon processing of personal data, between persons subject to proceedings, suspects, accused, injured parties, witnesses, imprisoned persons, detained persons, probationers and other persons as different categories of data subjects.

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

No, there are not.

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

No, there are not.

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

No, there are not.

8.1.3 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)?

1. Article 4 states that personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, in particular disclosed in the media, if there is public interest therefor and this is in accordance with the principles of journalism ethics. Disclosure of personal data must not cause excessive damage to the rights of any data subjects;

2. Article 5 states that personal data may be processed without the consent of the data subject for the purpose of academic, artistic and literary expression, in particular disclosed if this does not cause excessive damage to the rights of the data subject;

3. Article 6 states regulation about processing of personal data for needs of scientific and historical research and official statistics (for further details, please see answer to the question "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?");

4. Article 7 states that if personal data are processed for the purpose of archiving in the public interest, the controller or processor may restrict the rights of the data subject provided for in Articles 15, 16 and 18-21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the

achievement of the purpose of archiving in the public interest impossible or impedes it to a significant extent. The rights of data subjects specified in the last sentence may be restricted in order not to endanger the condition, authenticity, reliability, integrity and usability of the records.

5. Article 8 regulates processing of children's personal data for provision of information society services (for further details, please see an answer to question below).

6. Article 9 regulates processing of personal data after death of data subject (for further details, please see an answer to question below).

7. Article 10 regulates processing of personal data in connection with violation of obligation. This Article states that transmission of personal data related to violation of any obligation to third parties and processing of the transmitted data by any third party is permitted for the purpose of assessment of the creditworthiness of the data subject or for any other similar purposes and only in the case the controller or processor has verified the accuracy of the data transmitted and the legal basis for transmission of personal data and registered the data transmission.

Collection and transmission of data to third parties for the purposes specified in previous sentence is not permitted if: i) special categories of personal data are processed for the purposes of Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council; ii) these are data concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter; iii) it would excessively damage the rights or freedoms of the data subject; iv) less than 30 days have passed from the violation of a contract; v) more than five years have passed from the end of the violation of an obligation.

8. Article 11 regulates processing of personal data in public places. It states that unless otherwise provided by law, upon making in public places of audio or visual recordings intended for future disclosure, the consent of data subjects shall be substituted by an obligation to notify the data subjects thereof in a manner which allows the persons to understand the fact of the recording of the audio or visual images and to give the persons an opportunity to prevent the recording of their person if they so wish. The notification obligation does not apply in the case of public events, recording of which for the purposes of disclosure may be reasonably presumed.

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

Article 8 of PDPA states that if Article 6(1)(a) of GDPR applies in connection with provision of information society services directly to a child, processing of the child's personal data is permitted only in the case the child is at least 13 years old. If the child is below the age of 13 years, processing of personal data is permitted only in the case and to the extent for which consent has been given by the legal representative of the child.

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

No, there is no other vulnerable individuals identified.

8.1.4 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 Article 9 of PDPA regulates processing of personal data after death of data subject.

The consent of a data subject shall remain valid during the lifetime of the data subject and for 10 years after the death of the data subject, unless the data subject decided otherwise. If the data subject died as a minor, his or her consent shall be valid for the term of 20 years after the death of the data subject. The consent is not required if the processed personal data only contain the data subject's name, sex, date of birth and death, the fact of death, and the time and place of burial.

After the death of the data subject, processing of his or her personal data is permitted only with the consent of the successors of the data subject, except in the case: i) 10 years have passed since the death of the data subject; ii) 20 years have passed since the death of a data subject who was a minor; or iii) personal data are processed under any other legal bases. In the case of several successors, processing of the personal data of the data subject is permitted with the consent of any of them.

8.1.5 Accountability and Data Protection Impact Assessment

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

No, our national regulation does not introduce further provisions related to general accountability.

(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?

No, our national regulation does not specify data protection impact assessments requirements. Data processing in research is explained in previous questions.

8.2 Commercialization of data

8.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation	Brief description and scope
Regulation (EU) No 2016/679 (GDPR)	Regulation (EU) No 2016/679	Hard law	This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
Personal Data	Personal Data Protection Act	Hard law	1. Protection of natural persons upon processing of personal data to the extent in which it

Protection Act (PDPA)			elaborates and supplements the provisions contained in Regulation (EU) 2016/679; 2. Protection of natural persons upon processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments; 3. Supervision and formation of independent supervisory authority (Estonian Data Protection Inspectorate); 4. Liability for the violation of the requirements for processing of personal data. This Act provides for: i) standards for implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council; and ii) standards for transposition of Directive (EU) 2016/680 of the European Parliament and of the Council.
Law of Obligations Act (LOA)	Law of Obligations Act	Hard Law	The provisions of the General Part of this Act apply to all contracts specified in this Act or other Acts, including employment contracts and other multilateral transactions, contracts which are not regulated by law but are not in conflict with the content and spirit of the law, and obligations which do not arise from a contract.
Population Register Act (PRA)	Population Register Act	Hard Law	This Act provides for the composition of data in the population register and the procedure for the maintenance of the population register, entry of data on residence in the population register, provision of personal identification code, processing of data, ensuring access to data and exercise of supervision over such activities.

Copyright Act (CA)	Copyright Act	Hard Law	This Act regulates the rights of makers of databases and conditions for the exercise and protection.

Main regulatory tools addressing data commercialization in Estonia.

8.2.2 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, Estonia allows contracts based on exchange of personal data for services (for instance, to gain access to an app).

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

To our knowledge, yes, these are routinely performed.

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

No, there are no any specific regulation on the renumeration of data subjects if profit is made out of their data.

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

Yes, PIA regulates the secondary use of public information. Upon giving information for public use, the inviolability of the private life of persons, protection of copyrights, protection of national security, and protection of business secrets and other restricted information must be ensured. Before giving information for public use, the holder of information shall assess the need to establish restrictions on the public use of the information.

Additionally, in regards population register, there is particular national regulation, i.e. PRA.

The population register is a database which unites the main personal data on Estonian citizens, citizens of the European Union who have registered their residence in Estonia and aliens who have been granted a residence permit or right of residence in Estonia. The register is maintained and developed by the Ministry of the Interior, as the chief administrator of the register (for general overview please see Ministry of the Interior website).

One of the purposes of maintenance of the population register is also granting of access to personal data to legal persons and natural persons with legitimate interest for re-use of information in the population register.

The legal or natural person must pay state fee in accordance with State Fees Act prior to submitting an application with the reasoning of the planned usage of requested data.

Access to data is allowed only if this does not breach the inviolability of private life or endanger national security and if there is legitimate interest, access is allowed to data to which no access restrictions have been established.

8.2.3 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?

In different regulations, data is classified as personal data, public data, environmental data, spatial data, technical data, statistical data, meta data, micro-data, macro-data, etc.

The regulations do not specify that is data a product/commodity/good or service.

(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?

CA regulates the rights of makers of databases and conditions for the exercise and protection. There are no specific mechanisms to determine the value of data stated in regulations.

8.3 Security and cybersecurity

8.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Cybersecurity Act (CSA)	Cybersecurity Act	Hard Law	This Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.
Personal Data Protection Act (PDPA)	Personal Data Protection Act	Hard law	Article 43 states Security measures of processing of personal data by law enforcement authorities in prevention, detection and proceedings of offences and execution of punishments
Public Information Act (PIA)	Public Information Act	Hard Law	Article 43 of this Act states general regulation for protection of internal information to a holder of information. Article 43[9] (1) (4) refers to the system of security

			measures for information systems.
Security Measures for Information Systems Regulation (SMISR)	Infosüsteemide turvameetmete süsteem	Hard Law	This Regulation states a system of security measures for the information systems used for processing the data contained in state and local government databases and related information assets.
Emergency Act (EA)	Emergency Act	Hard Law	Article 41 (1) of this Act states that a provider of a vital service shall comply with the requirements provided by and on the basis of §§ 7 and 8 of the Cybersecurity Act to ensure the security of the network and information system used for the provision of the vital service.
Information Security Management System of Government Authorities (ISMSGA)	Infoturbe juhtimise süsteem	Hard Law	This Regulation regulates information security management system of government authorities.

Main regulatory tools addressing security and cybersecurity in Estonia

8.3.2 Implementation of EU Law

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

Please see the table above.

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

Estonia has transposed the NIS directive. For further details, please see CSA.

(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?

Yes, this prevention is reflected in national regulation, mostly stated as principles (i.e. technical and organisational measures are not stated in detail).

8.3.3 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?

Additionally, to the GDPR's general notification requirement, if there is a personal data breach during processing of personal data by law enforcement authorities, and the personal data breach is likely to entail a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the Estonian Data Protection Inspectorate of the breach, if possible, within 72 hours after becoming aware thereof. Additionally, when a breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the data subject of the personal data breach.

Cybersecurity Act (which implements the NIS Directive) does not state special regulation to Personal Data Breach Notification.

8.3.4 Supervision of cybersecurity

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

in Cybersecurity Act and in legislation established on the basis of this Act are exercised by the Estonian Information System Authority. The up-to-date Statutes of this authority is stated in Estonian and older version is also available in English.

Systems necessary for international military cooperation within the area of government of the Ministry of Defence is supervised by the Ministry of Defence and the Estonian Defence Forces.

(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?

As stated in previous answer, the Estonian Information System Authority fulfils the obligation as cyber security authority, i.e. it develops cyber security strategies and policies, coordinates the safe implementation of IT infrastructures important for the state and conduct supervision and monitors the Estonian computer network and solve cyber incidents.

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

Damages caused by lack of cybersecurity can be claimed (and compensated) accordingly to the ordinary claim for damages, i.e. there is not stated specific regulation about claiming damages related to cybersecurity.

8.4 Enforcement: fines and sanctions

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

Yes, Penal Code (**PE**) states the following:

1. Article 157[1] of PE states that illegal disclosure of specific categories of personal data, data concerning commission of offence or falling victim to offence is punishable by a pecuniary punishment or up to one year's imprisonment.
2. Article 157[2] of PE states that illegal use of another person's identity is punishable by a pecuniary punishment or up to three year's imprisonment.
3. PE also states several crimes related to cybersecurity and these are also punishable by a pecuniary punishment or up to three year's imprisonment.

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

Upon failure to comply with a precept of the Estonian Data Protection Inspectorate, the upper limit of the penalty payment (i.e. coercive measure in the meaning of Substitutive Enforcement and Penalty Payment Act) is up to 20,000,000 euros, or in the case of undertakings up to 4 per cent of the total global annual turnover of the undertaking for the previous financial year, whichever amount is the higher. The application of a coercive measure is not deemed to be a punishment.

In misdemeanour procedure conducted by Estonian Data Protection Inspectorate, violation of obligations stated in Articles 62 to 72 of PDPA and in GDPR are punishable by a fine up to 20,000,000 euros or up to 4 per cent of processors total global annual turnover for the previous financial year, whichever amount is the higher (in accordance with Article 83 of GDPR).

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

Data protection offences constitute an official offence.

8.5 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?

It is regulated in Article 6 of PDPA, which regulates processing of personal data for needs of scientific and historical research and official statistics as follows:

(1) Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provides equivalent level of protection. Prior to transmission of

personal data for processing for the needs of scientific and historical research or official statistics, personal data shall be replaced by pseudonymised data or data in a format which provides equivalent level of data protection.

(2) Depseudonymisation or any other method by which the data not enabling identification of persons are changed again into the data which enable identification of persons are only permitted for the needs of additional scientific and historical research or official statistics. Processors of personal data shall designate a person identified by name who has access to the information allowing pseudonymisation.

(3) Processing of data concerning any data subjects for the needs of scientific and historical research or official statistics without the consent of the data subject in a format which enables identification of the data subject is permitted only in the case the following conditions are met:

1) the purposes of data processing can no longer be achieved after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes;

2) there is overriding public interest for it in the estimation of the persons conducting scientific and historical research or compiling official statistics;

3) the scope of obligations of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner.

(4) If scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.

(5) For the purposes of this Act, scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development. In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided for in this section, except in the case the objectives of the studies conducted for policy development and the scope of processing of personal data derive from legislation.

(6) Where personal data are processed for the purpose of scientific and historical research or official statistics, the controller or processor may restrict the rights of data subjects provided for in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the achievement of the objectives of the scientific and historical research or official statistics impossible or impedes it to a significant extent.

(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?

Yes, for example, Research Ethics Committee of the University of Tartu (for detailed information, please see answer on page 10 of this questionnaire) asks the applicant to analyse the ethics question in the application of the research. The ethics committee shall assess the ethics side and the compliance with the conditions stated in Article 6 of PDPA. There is no software for data protection impact assessment and the guideline referred at the end of page 9 of this questionnaire is out-dated, therefore there is no valid guideline from the Estonian Data Protection Inspectorate as well.

(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?

No, there are not 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

9 Finland

Erkko Korhonen (Hannes Snellman Attorneys Ltd)

9.1 Informed consent

9.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope
Suomen perustuslaki (731/1999, as amended) ***The Constitution of Finland*** **(“Constitution”)**	https://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf	Hard law with the constitutional status	Establishes everyone’s fundamental right to privacy and sets the basis for all other legislation (Section 10)
Tietosuojalaki (1050/2018) ***Data Protection Act*** **(“FDPA”)**	https://www.finlex.fi/fi/laki/kaannokset/2018/en20181050.pdf	Hard law	Supplements and makes national derogations to the GDPR
Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen	https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf	Hard law	Applies to the processing of personal data by competent authorities in the context of criminal matters