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

yhteydessä (1054/2018, as amended) ***Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security* (“CFDPA”)**			
Laki yksityisyyden suojasta työelämässä (759/2004, as amended) **Act on the Protection of Privacy in the Working Life (“PWLA”)**	https://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf	Hard law	Contains specific provisions on the processing of personal data in the context of employment
Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019), ***Act on Secondary Use of Social and Welfare Information***	https://www.finlex.fi/fi/laki/alkup/2019/20190552 (only available in Finnish)	Hard law	Aims to ensure the secure processing of personal data in social and welfare related activities when the secondary use of the personal data relates to control, monitoring, research and statistical measures.
Laki sähköisen viestinnän palveluista (917/2014, as amended) ***Act on Electronic Communications Services* (“ECSA”)**	https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf (amendments only up to 917/2014 included) https://www.finlex.fi/fi/laki/ajantasa/2014/20140917	Hard law	Aims to ensure the confidentiality of electronic communication and the protection of privacy

	(up-to-date Finnish version)		
Laki viranomaisten toiminnan julkisuudesta (621/1999, as amended) ***Act on the Openness of Government Activities*** **("AOGV")**	https://www.finlex.fi/fi/laki/kaannokset/1999/en19990621_20150907.pdf (amendments only up to 907/2015 included) https://www.finlex.fi/fi/laki/ajantasa/1999/19990621 (up-to-date Finnish version)	Hard law	Contains provisions on the right of access to official documents in the public domain, officials' duty of non-disclosure, document secrecy and any other restrictions of access that are necessary for the protection of public and private interests

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

(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?

Yes, Section 10 of the Constitution establishes the fundamental right to privacy and stipulates that everyone's private life, honour and the sanctity of the home shall be guaranteed. However, the national legislation implementing and supplementing the GDPR does not contain any specific provisions that would extend the scope of the GDPR.

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

Concerning the national security, the main regulatory tool is the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security ("CFDPA"). The Act applies to the processing of personal data by competent authorities in the context of criminal matters as well as when the processing is carried out in performing such a duty that is related to the protection of national security (Section 1 of the CFDPA). For example, the Act stipulates that the rights of the data subject may be restricted in certain situations, if these restrictions are, considering the rights of the data subject, proportionate and necessary in order to protect national security (Section 26 of the CFDPA).

Name of Authority	Link (English version if possible be)	Is this an indepe	Number of employees	Level of activity (according to your	Response to requirements, questions,

		ndent body?		appreciation)?	etc. made by the public
Tietosuojavaltuutettu ***Data Protection Ombudsman***	https://tietosuoja.fi/en/home	Yes	40	Not that active. Not a single fine has been imposed yet by the Sanctions Board operating under the Ombudsman's office.	Telephone guidance available during the weekdays. The Ombudsman has some guidance on the GDPR on its website.

Information regarding Data Protection Authority, Finland

(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, the term "*data processing for research" purposes* is used but not specifically defined in the FDPA.

Pursuant to Section 31 of the FDPA, the controller may restrict some data subject rights if the personal data is processed for scientific or historical research or statistical purposes. Such derogations to data subject rights require, for example, that the processing for such research purposes is based on an appropriate research plan and that there is an assigned person or a group to be in charge of the research.

The term *research in public interest* is not defined either.

Pursuant to Section 4 of the FDPA, processing of personal data may be based on Article 6(1)(e) of the GDPR if "*[...]* 3) the processing is necessary for scientific or historical research purposes or statistical purposes, and it is proportionate to the legitimate interest pursued in the public interest; or 4) the processing of personal data included in research material, cultural heritage material, and descriptions of such material for archiving purposes is necessary and proportionate in relation to the aim pursued in the public interest and for data subjects' rights."

According to the Government Proposal (HE 9/2018 vp), the provision would not seek to define the scope of use that results from *archiving in the public interest*, which is ultimately determined by the interpretation of the CJEU. In any event, "*archiving in the public interest*" may also be considered to cover other processing of the documentation and not just preservation. Archiving in the public interest generally involves at least organizing data, defining metadata and combining data.

(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, the Section 31 of the FDPA mainly implements Article 89 of the GDPR to the national legislation. Pursuant to Section 31, where necessary in the context of processing of personal data for scientific or historical research purposes, data subject rights which are based on Articles 15, 16, 18, and 21 of the GDPR may be restricted if the following preconditions laid down in the FDPA are met:

1) the processing is based on an appropriate research plan;

2) a person or a group has been assigned to be in charge of the research; and

3) personal data are used and disclosed only for scientific or historical research purposes or for some other compatible purpose and, it is also ensured in other situations, that information relating to a specific person are not disclosed to third parties.

In addition, when special categories of personal data or data relating to criminal convictions and offences are processed for scientific or historical research or statistical purposes and the controller decides to restrict the rights of a data subject under the above provisions of Section 31 of the FDPA, a data protection impact assessment must be conducted or applicable Article 40 of the GDPR "Codes of Conduct" be complied with. In case a data protection impact assessment is conducted, it must be submitted to the Office of the Data Protection Ombudsman at least thirty days before commencing the envisaged processing

(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, there are no specific safeguards mentioned that would go beyond Article 9 of the GDPR and the appropriate safeguards depend on a case-by-case basis. In Finnish law, Article 9 of the GDPR is implemented so that Section 6(1) of the FDPA defines some situations where the GDPR Article 9(1) does *not* apply. These relate to situations where insurance institutions are processing certain health data, processing that is provided by law, processing of data concerning trade union membership when necessary, and processing by a healthcare service provider when arranging or producing services. In addition, the list includes processing by a social welfare service producer when arranging or producing services or granting benefits, processing in anti-doping work and sports for persons with disabilities when necessary, processing for scientific, historical or statistical purposes, and processing of research and cultural heritage materials for archiving purposes in the public interest, with the exception of genetic data

Section 6(2) of the FDPA, on the other hand, requires appropriate and special safeguards to be used for protecting data subjects' rights in the situations mentioned in the first paragraph. Such measures include

1) measures by which it is possible to afterwards verify and prove who has saved, amended or transferred personal data;

2) measures by which the competence of the personnel processing personal data are improved;

3) designation of a data protection officer;

4) internal measures of the controller and processor by which it is possible to prevent access to personal data;

5) pseudonymisation of personal data;

6) encryption of personal data;

7) measures to safeguard continuous confidentiality, integrity, usability, and resilience of the processing systems and services relating to processing of personal data, including the ability to restore the availability of and access to data, in case of a physical or a technical failure;

8) measures to test, study and evaluate the effectiveness of technical and organisational measures for ensuring the safety of data processing;

9) special procedure rules to ensure the compliance with the GDPR and the FDPA when transferring personal data and when processing personal data for other purposes;

10) undertaking a DPIA as set out in Article 35 of the GDPR

According to the Government proposal (HE 9/2018 vp) the safeguards listed in Section 6(2) are "in compliance with the GDPR". Yet, it must be noted that the list of safeguards in Section 6(2) of the FDPA is not exhaustive nor mandatory, but is to be considered an example list of possible safeguards. The controller shall evaluate the risks of the processing of the personal data and apply appropriate safeguards accordingly, which may also include other safeguards than those included in the list.

(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.)?

According to our knowledge, there are no national Codes of Conducts established specifically for the ethics of data processing in research. However, there exist a number of bodies for ethics in research and ethics in general. Also the Government Proposal (HE 9/2018 vp) mentions that research containing sensitive data shall particularly comply with generally accepted principles of research ethics. For example, the Finnish National Board on Research Integrity (TENK) , address ethical questions relating to research and to the advancement of research ethics in Finland.

In 2019, TENK released guidelines on "The ethical principles of research with human participants and ethical review in the human sciences in Finland" which are also available in English. Section 3.5 of the said guidelines addresses the question of processing of personal data in research: The central principles for processing research data containing personal data are that this must be planned, responsible and in accordance with the law. Planning must include appropriate consideration of the risks associated with the processing of research data to the research participants and others. The duty of responsibility applies to the entire lifespan of the research data and the study. The researcher must comply with the legislation in force and with the research-related data protection guidelines issued by their own organisation. Decisions made regarding the processing of personal data must be justified and clearly documented. Decisions made must be able to be checked subsequently by the authorities or the data protection officer of the organisation.

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

There is no specific definition of "statistical purposes" in the Finnish FDPA.

Pursuant to Section 31(2) of the FDPA, the controller may restrict the data subject rights which are based on Articles 15, 16, 18, and 21 of the GDPR when personal data are processed for statistical purposes, if the following conditions are met:

1) statistics may not be produced or the requirement for information may not be fulfilled without processing of personal data; 2) producing the statistics has a material connection with the activities of the controller; and; 3) information is not disclosed or made available in a way that a specific person is identifiable from the information, unless it is disclosed for public statistics.

Again, it must be noted that when special categories of personal data or data relating to criminal convictions and offences are processed for statistical purposes and the controller decides to restrict the rights of a data subject under the above provisions of Section 31 of the FDPA, a data protection impact assessment must be conducted or applicable Article 40 of the GDPR "Codes of Conduct" be complied with. In case a data protection impact assessment is conducted, it must be submitted to the Office of the Data Protection Ombudsman at least thirty days before commencing the envisaged 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.)

As mentioned above, Section 31(3) of the FDPA contains such additional duties. According to the Section 31(2), when special categories of personal data or data relating to criminal convictions and offences are processed for scientific or historical research or statistical purposes and the controller decides to restrict the rights of a data subject under the above provisions of Section 31 of the FDPA, a data protection impact assessment (DPIA) must be conducted or applicable Article 40 of the GDPR "Codes of Conduct" be complied with. In case a data protection impact assessment is conducted, it must be submitted to the Office of the Data Protection Ombudsman at least thirty days before commencing the envisaged processing.

In addition, there are some sectors specific regulation, for example in the field of medical research. According to Section 6 of the Medical Research Act (488/1999, as amended, Finnish: laki lääketieteellisestä tutkimuksesta), medical research on persons may not be conducted without the research subject's informed consent in writing. Research subjects shall be entitled to withdraw their consent at any point prior to the completion of the research. The Section 6a of the Act further regulates the processing of personal data in the medical research after the consent has been withdrawn. If the data subject has withdrawn its consent, the processing of personal data is only possible to the extent it is necessary in order to determine or evaluate the purpose, properties, effects, efficacy or safety of the medicinal product, medical device. In addition, it is required that the subject knew when giving consent that the data collected prior to the withdrawal of consent would be processed as part of the study material.

9.1.2 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.)

No, the Finnish FDPA applies within the scope of application of Article 2 of the Data Protection Regulation. Data subjects are considered as natural persons

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

Although not specifically defined in the FDPA, the definition of data subject's informed consent is regarded as complying with the GDPR. The consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes.

However, pursuant to Section 5 of the FDPA, the applicable age of consent in relation to information society services offered directly to a child is 13 years whereas according to the GDPR the child must be at least 16 years old.

The age limit of 13 years only applies to consent given in relation to information society services offered directly to a child. If a consent needs to be obtained for the processing of any other nature, the applicable age of consent is determined in accordance with the general rules of the Finnish Act on Child Custody and Right of Access (361/1983). The general rule is that the person having custody of a child represents the child in matters concerning his or her person, unless otherwise provided by the law. The child can however represent him/herself (including give a consent) in matters that are considered appropriate taking into account the child's age. As a rule of thumb, a 15-year-old may generally represent him/herself in "ordinary matters", such as to give consent to the use of photographs or for direct marketing purposes

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

Overall, there are no special requirements regarding, for example, legislation restricting data processing. However, certain restrictions to processing are provided in the FDPA and sector-specific legislation, e.g. in the healthcare sector and for the processing of credit information.

Chapter 2 of the FDPA concerns the legal basis for data processing in certain cases. It elaborates the articles of the GDPR and makes exceptions on a national level. Section 4 of the FDPA specifies processing that is carried out in the public interest or in the exercise of official authority vested in the controller. Section 5 sets special requirements for the processing of children's personal data and section 6 restricts the processing of special categories of data (more in part I, section 3 of this report). In addition, section 7 of the FDPA includes exemptions from the article 10 of the GDPR. These exceptions are: when processing data relating to criminal convictions and offices or related security measures referred to in Article 10, the data may be processed only if the processing is necessary for the investigation, establishment, exercise, defence or resolution of a legal claim or if the data is processed for certain purposes referred to in section 6. The data controller and processor shall take appropriate and special safeguards if an above-mentioned situation is at hand. Section 6 subsection 2 includes a list of such measures.

As regards the processing of employee personal data, the Act on Protection of Privacy in Working Place governs (together with the GPDR and FDPA) the processing of personal data in the employment context.

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

Fulfilling the data subject's rights is always the main rule. If the data controller declines the data subject's request, there must always be a legal basis for the rejection. In addition to the GDPR's exceptions to the data subject's rights, the FDPA includes certain limitations to the data subject's rights. Section 31 concerns personal data that is processed for scientific, historical and statistical purposes. According to the section, the

data subject's rights may be derogated from in certain circumstances (mentioned above in part I section 1).

On the other hand, section 34 includes three restrictions concerning the right of access. Firstly, the data controller may decline the data subject's request if providing access to the data could compromise national security, defence, or public order and security, or hamper the prevention or investigation of offences. The second restriction concerns a situation when providing access to the data could seriously endanger the health or treatment of the data subject or the rights of some other person. Third, access should not be given if the personal data is used in the performance of supervisory and inspection tasks and the refusal to provide access to the data is necessary to safeguard an important economic or financial interest of Finland or the European Union. However, since the data subject's rights are always the main rule, if an above-mentioned situation applies only to a part of the data, the data subject has the right of access to the remainder of the data concerning him or her.

9.1.3 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)?

Section 6 of the FDPA concerns the processing of special categories of personal data, implementing the Article 9(1) of the GDPR (see part I section 1 for more). There is no definition for special categories of data in Section 6 of the FDPA; it only contains guidance on when article 9(1) does not apply and regulates appropriate safeguards. In the section 6 of the FDPA, there is a list of situations where the GDPR article 9(1) does not apply. These situations include insurance institutions processing certain health data, processing that is provided by law, processing of data concerning trade union membership when necessary, and processing by a healthcare service provider when arranging or producing services. In addition, the list includes processing by a social welfare service producer when arranging or producing services or granting benefits, processing in anti-doping work and sports for persons with disabilities when necessary, processing for scientific, historical or statistical purposes, and processing of research and cultural heritage materials for archiving purposes in the public interest, with the exception of genetic data.

As set out in Section 6 of the FDPA, the data controller and processor shall take appropriate and special safeguards if an above-mentioned situation is at hand. Subsection 2 includes a list of such measures. Thus, specific categories, e.g. data of legal entities, is not mentioned.

Further, the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security ("CFDPA") contain provisions on processing of special categories of data. According to Section 11 of the Act, the processing of special categories of personal data is allowed only where it is strictly necessary, subject to appropriate safeguards for the rights of the data subject, and only where the processing 1) is provided by law; 2) relates to the consideration of a criminal case in the prosecution service or in court; 3) is necessary for protecting a vital interest of the data subject or of another natural person; or 4) relates to data which the data subject has manifestly made public. In addition, according to Section 11(3) of the Act, profiling that results in discrimination against natural persons on the basis of special categories of personal data is prohibited.

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

Pursuant to Section 5 of the FDPA, the applicable age of consent in relation to information society services offered directly to a child is 13 years.

The age limit of 13 years only applies to consent given in relation to information society services offered directly to a child. If a consent needs to be obtained for the processing of any other nature, the applicable age of consent is determined in accordance with the general rules of the Finnish Act on Child Custody and Right of Access (361/1983). The general rule is that the person having custody of a child represents the child in matters concerning his or her person, unless otherwise provided by the law. The child can however represent him/herself (including give a consent) in matters that are considered appropriate taking into account the child's age. As a rule of thumb, a 15-year-old may generally represent him/herself in "ordinary matters", such as to give consent to the use of photographs or for direct marketing purposes

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

The Finnish FDPA does not contain special provisions for other potentially vulnerable groups.

9.1.4 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?

In Finland, in principle the fundamental rights of a person cease upon the person's death, and the personal data of deceased individuals therefore loses the direct protection under the Finnish FDPA. However, the privacy rights of living friends or relatives of the deceased still have to be respected. For example, the information of a genetic disease of the deceased individual may also be considered as personal data of the relatives of this individual. The rights of the deceased individuals may also be protected indirectly through provisions relating to defamation.

In addition, under the previous law regulating data protection in Finland (repealed Personal Data Act, 523/1999, as amended, Finnish: henkilötietolaki), the Finnish Data Protection Board (Tietosuojalautakunta) had prohibited the processing of personal data of a deceased person in a case where the processor had obtained the personal data from the tombstone and processed it in automated open network without obtaining the consent from the deceased individual's right holders.

9.1.5 Accountability and Data Protection Impact Assessment

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

To our knowledge, there are no further provisions, requirements or procedures in the Finnish legislation.

(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?

As already stated above, when special categories of personal data or data relating to criminal convictions and offences are processed for scientific or historical research or statistical purposes and the controller decides to restrict the rights of a data subject under the provisions of Section 31 of the FDPA, a data protection impact assessment must be conducted or applicable Article 40 of the GDPR "Codes of Conduct" be complied with. In case a data protection impact assessment is conducted, it must be submitted to the Office of the Data Protection Ombudsman at least thirty days before commencing the envisaged processing.

9.2 Commercialization of data

9.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Kuluttajansuojalaki (38/1978, as amended) ***Consumer Protection Act***	https://www.finlex.fi/fi/laki/kaannokset/1978/en19780038_20050029.pdf (amendments only up to 29/2005 included) https://www.finlex.fi/fi/laki/ajantasa/1978/19780038 (up-to-date Finnish version)	Hard law	The Act applies to the offering, selling and other marketing of consumer goods and services by businesses to consumers. The Act includes regulation of contract terms.
Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) ***The Act on the Secondary Use of Social and Health Data***	https://www.finlex.fi/fi/laki/alkup/2019/20190552 (only in Finnish)	Hard law	The Act concerns processing social and health data for statistical and scientific purposes, development and innovation activities etc., when the data was originally gathered for another purpose.

Main regulatory tools addressing data commercialization in Finland.

9.2.2 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)?

There are no specific regulations for the contractual exchange of personal data as a payment for services. However, restricting such contracts is possible under the Consumer Protection Act. According to Section 1 of Chapter 3, companies may not use terms that are unreasonable for the consumer. For example, according to legal praxis, unclear and misleading terms may be considered unreasonable. Thus, in Finland exchange of personal data for services may be forbidden if the contract does not fulfil the requirements of consumer protection.

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

Stipulations about the processing of personal data are routinely contained in the terms of service of companies. However, the personal data must be processed in accordance with the FDPA and GDPR, and relations between companies and consumers shall comply with Consumer Protection Act.

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

There is no such regulation in Finland.

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

The FDPA does not include provisions that would limit the application of the purpose limitation principle as set out in Article 5(1)(b). Therefore, the purpose limitation principle of the GDPR applies in all circumstances. However, Article 6(4) of the GDPR, which sets out the requirement of a compatibility assessment, does not apply when personal data is processed under Section 27 of the FDPA solely for journalistic, academic, artistic, and literary expression purposes.

However, we do have other regulation on the secondary use of data, namely the Act on the Secondary Use of Social and Health Data. The Act concerns processing social and health data for statistical and scientific purposes, development and innovation activities, education, knowledge management, the guidance and supervision of social and healthcare authorities, as well as authorities' planning and clearing functions, when the data was originally gathered for another purpose. The goal of the act is to enable efficient and secure processing of personal data in above-mentioned activities. In addition, the goal is to ensure the legitimate expectations and rights of data subjects.

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

No.

9.2.3 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 Finland, data is not classified in any legal category. However, data may have a different nature in different contexts. For example, data containing trade secrets of companies is protected under the Trade Secret Act (595/2018, Finnish: liikesalaisuuslaki). On the other hand, if data is organized in a creative way, it may be protected as a database under the Copyright Act (404/1961, as amended, Finnish: tekijänoikeuslaki). Thus, data does not have an independent legal status in Finland.

(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?

Data that constitutes a work of art is protected under the Copyright Act. A mechanism to determine the value of data can be found in Section 26a of the Copyright Act. The State shall pay compensation to the authors of the work that was reproduced for private use. The amount of compensation shall be settled at a level that may be considered a fair compensation for the reproduction. The reproduction and its frequency are surveyed in order to determine the right amount of compensation. The survey is conducted by an independent research institution approved by the Ministry of Education and Culture.

Additionally, data may be protected under the Trade Secret Act. According to Section 10, the person who has obtained, disclosed or used a trade secret unlawfully must pay compensation for the use in certain cases. The compensation shall not exceed the amount of license payments and other payments the person should pay if he/she would gain permission for the use for the time period during which the use could be prohibited. In addition, Section 11 concerns compensation for damages. If a person intentionally or negligently uses a trade secret unlawfully, he/she shall pay a fair compensation to the holder of the trade secret for using the trade secret and for all damages the offense causes.

The mechanisms described in this Section may determine the value of data in very specific situations and they do not constitute a general rule. In Finnish legislation, there are no general mechanisms to calculate the value of data.

9.3 Security and cybersecurity

9.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Laki sähköisen viestinnän palveluista (917/2014, as amended) Act on Electronic Communications Services "ECSA"	https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf (amendments only up to 917/2014 included) https://www.finlex.fi/fi/laki/ajantasa/2014/20140917) (up-to-date Finnish version)	Hard law	The act concerns the supply and use of electronic communications services. Among other things, the goal of the act is to ensure that communications networks and services are technologically advanced, of high quality, reliable, safe, and inexpensive.
Laki vahvasta sähköisestä	https://www.finlex.fi/fi/laki/kaannokset/2009	Hard law	The act concerns strong electronic

tunnistamisesta ja luottamuspalveluista (617/2009, as amended) ***Act on Strong Electronic Identification and Trust Services***	/en20090617_20090617.pdf (amendments only up to 617/2009 included) https://www.finlex.fi/fi/laki/ajantasa/2009/20090617) (up-to-date Finnish version)		identification and trust services for electronic transactions in the internal market.

Main regulatory tools addressing security and cybersecurity in Finland

9.3.2 Implementation of EU Law

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

No.

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

The NIS directive has been implemented to several Finnish laws, including the ECSA, by the Government Degree HE 192/2017. Other laws that were subject to amendments due to the implementation process included, for example, Aviation Act, Act on Transport Services, Electricity Market Act and Act on the Financial Supervisory Authority. The implemented legislation entered into force on 9 May 2018.

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

According to the Office of the Data Protection Ombudsman, technical and organisational measures refer to, for example, instructions given to staff to ensure data protection, internal checks on use, the security of information systems, data encryption and other security measures. However, Finnish legislation does not specify any technical and organisational measures. Instead, the FDPA includes provisions on appropriate technical and organisational measures in specific situations, such as processing special categories of data in accordance with Section 6 (more in part I, section 3 of this report).

(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.

9.3.3 Personal Data Breach Notification

(ii) 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?

In Finland, the supervisory authority referred to in the GDPR is the Data Protection Ombudsman. Thus, in accordance with the GDPR, the data protection ombudsman should

be notified of a data breach within 72 hours after the controller has become aware of the personal data breach. The notification should be made using the data breach notification form on the website of the Office of the Data Protection Ombudsman or, if the notification includes sensitive or confidential information, the Ministry of Justice's secure e-mail.

NIS Directive has been implemented to different Finnish laws. Critical infrastructure providers and essential digital service providers are obliged to report security incidents to the supervisory authority in their sector. The notification obligation applies to energy, digital infrastructure, digital services, financial, financial infrastructure, transport, health and water supply sectors. Amendments have been made to the respective laws that regulate these sectors.

For example, Sections 274 and 275 of the ECSA concern notifications of significant data breaches. Section 274 concerns a tele company's obligation to notify the subscriber and user if its service is threatened by or has experienced a significant data breach or some other event that impedes the functions of the communications service or disturbs it substantially. In addition, section 275 concerns the obligation to notify the Finnish Transport and Communications Agency in the same type of situation. Section 275 is derived from the NIS Directive.

9.3.4 Supervision of cybersecurity

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

The National Cyber Security Centre (NCSC-FI)[78] steers and supervises compliance with the regulations that apply to its field of activity, and it provides support and assistance to maintain and develop cybersecurity. The functions of the NCSC-FI are regulated in the Section 3 of the Act on Finnish Transport and Communications Agency (935/2018).

The NCSC-FI at Finnish Transport and Communications Agency (Traficom) is the appellate authority in several matters. If a problem cannot be settled by means of guidance or negotiations, Traficom settles the matter in an administrative procedure and issues a decision, which is then subject appeal, if needed. Such decision may be required, for example, if an operator subject to regulation has neglected or violated provisions and fails to correct its actions, or if a party needs a decision due to conflicting interests or differences in interpretation.[79]

(v) 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 mentioned in the previous question the NCSC-FI is the Finnish authority responsible for cybersecurity. It operates under the Finnish Transport and Communications Agency,

[78] National Cyber Security Centre webpage: https://www.kyberturvallisuuskeskus.fi/en

[79] For more information on NCSC-FI's powers and functions see their webpage which are also available in English: https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/how-we-regulate

Traficom.[80] According to the NCSC-FI, it has four main responsibilities: CERT(*Computer Emergency Response Team*), PRS (*Public Regulated Service*), regulation and supervision, and NCSA (*National Communications Security Authority*).

The purpose of the CERT activities is to prevent information security incidents and to disseminate information on information security matters. The Public Regulated Service (PRS) aims to provide secure and reliable position and timing information to public authorities and operators critical for the security of supply.

The NCSC-FI steers and supervises compliance with the regulations that apply to its field of activity. It coordinates and monitors provisions on information security, non-interference and confidential communications. It drafts regulations, recommendations and reports on these subjects while registering and monitoring related operators.[81]

In Finland, the responsibility for *international* information security obligations has been divided among several authorities. The overall responsibility for international information security obligations lies with the Ministry for Foreign Affairs. The Ministry acts as the National Security Authority (NSA) in Finland.[82] The NCSC-FI is a part of the Finnish security authority organisation as a National Communications Security Authority (NCSA). As the national information security authority the NCSC-FI is responsible for security matters related to the data transfer and handling of classified information in electronic communications. The services of the NCSA support organisations' proactive security work and operational possibilities.

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

The FDPA includes provisions on legal protection, but they do not concern actual claims for damages. According to the Office of the Data Protection Ombudsman, the Data Protection Ombudsman does not act as an attorney and cannot, for example, claim damages on your behalf. Civil claims must be filed with the courts.

The Tort Liability Act (412/1974, as amended, Finnish: vahingonkorvauslaki) is the general law for liability for damages, and the Code of Judicial Procedure (4/1734, as amended, Finnish: oikeudenkäymiskaari) includes general provisions on handling civil cases. Since there is no specific regulation for claiming damages for cybersecurity breaches, these are the general laws that apply to the case.

Class action lawsuits are available for consumers in Finland, and the relevant provisions are in the Act on Class Actions (444/2007, as amended, Finnish: ryhmäkannelaki). However, the applicability of the class action procedure is limited; for instance, the Consumer Ombudsman has exclusive standing to bring a class action to be heard in a court. Due to the narrow scope, class actions have never been used in Finland. However, in cybersecurity cases class actions could be a viable option for consumers: according to Section 17 of the Act on Class Actions, class members are not liable for the legal costs of the procedure.

[80] National Cyber Security Centre's website: https://www.kyberturvallisuuskeskus.fi/en/
[81] See NCSC-FI's website for more information re authority's powers
[82] National Security Authority's website: https://um.fi/national-security-authority

9.4 Enforcement: fines and sanctions

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

Chapter 38 of the Finnish Criminal Code (39/1889, as amended, Finnish: rikoslaki) concerns data and communications offences. Section 9 of said chapter concerns data protection offence. If someone other than a data controller or processor determined in the GDPR obtains personal data in a way that is incompatible with the purpose of the data's use, discloses personal data or transfers it against data protection laws, and thus offends the privacy of the data subject or causes them damage or substantial inconvenience, the person is guilty of a data protection offence. The penalty is a fine or up to a year of imprisonment. The offense is punishable both intentionally and through gross negligence.

Further, the punishments for a message interception and an aggravated message interception are laid down in Chapter 38, Sections 3 and 4 of the Finnish Criminal Code, and the punishments for a computer break-in and an aggravated computer break-in in Chapter 38, Sections 8 and 8a of the Finnish Criminal Code. The punishments for an infringement of the non-disclosure obligation (Section 35 of the FDPA) and for an infringement of the secrecy obligation (Section 36 of the FDPA) are imposed in accordance with Chapter 38, Section 1 or 2 of the Finnish Criminal Code. Most of these crimes may be punished by either a fine or an imprisonment.

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

Pursuant to Section 24 of the FDPA, the administrative penalty payment laid down in Article 83 of the GDPR (administrative fine) is imposed by a collegial body for sanctions (i.e. a Sanctions Board), which is composed of the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen. Decisions of the collegial body are made upon presentation. The collegial body has a quorum with three members present. Decisions shall be based on the opinion seconded by the majority. In case of a tie, the decision shall be based on the opinion that is more favourable for the party subject to the sanction.

An administrative fine may also be imposed for an infringement of Article 10 of the GDPR in compliance with the provisions of this Act and Article 83(5) of the Regulation. Provisions on the enforcement of an administrative fine are laid down in the Act on the Enforcement of Fines (672/2002).

An administrative fine cannot be imposed on public authorities such as central government authorities, state enterprises, municipal authorities and autonomous institutions governed by public law and churches.

In addition, pursuant to Section 22 of the FDPA, the Data Protection Ombudsman may impose conditional fines under for the purpose of enforcing an order referred to in points (c)–(g) and (j) of Article 58(2) of the GDPR and to enforce an order to provide information that has been issued under Section 18 of the FDPA.

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

Data protection offences, such as the one under Chapter 38 Section 9 of the Finnish Criminal Code constitute an official offence and the public prosecutor has the right to bring charges in data protection offences in accordance with Chapter 38 Sections 9 and 10 of the Finnish Criminal Code. The public prosecutor shall hear the Data Protection Ombudsman before bringing charges for a data protection offence.

9.5 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?

Concerning data protection and research ethics, the Government Proposal (HE 9/2018 vp) to the FDPA mentions that research containing sensitive data shall particularly comply with generally accepted principles of research ethics. However, to our knowledge, there are no general mandatory guidelines or regulations governing data protection issues in research projects.

Yet, in the field of medical research, there are some specific regulations, namely in the Medical Research Act and in the Biobank Act (688/2012, as amended, Finnish: biopankkilaki). For example, HUS (Hospital District of Helsinki and Uusimaa) has four Ethical committees that evaluate and give opinions on the ethics of medical research in the hospital district. The Medical Research Act governs the functions of the HUS Ethical committees.

In addition, as already mentioned above in Part I section I, the Finnish National Board on Research Integrity (TENK), addresses ethical questions relating to research and to the advancement of research ethics in Finland. TENK has released guidelines on “The ethical principles of research with human participants and ethical review in the human sciences in Finland”. The guideline also addresses the question of processing of personal data in research.

(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?

In principle, major research funding agencies in Finland do not have instruments to promote data protection. However, they do have data protection policies and their websites provide information on the requirements of the GDPR and the FDPA.

(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?

To our knowledge, there is no such regulation in Finland directly affecting such R&I activities. Obviously, in case dual-use technology is created and intended to be exported, the provisions on export restrictions must be complied with. In Finland, the Act on the Control of Exports of Dual-Use Goods (562/1996, as amended, Finnish: laki

kaksikäyttötuotteiden vientivalvonnasta) regulates the export controls of dual use items. The Ministry of Foreign Affairs is the national supervisory and licensing authority for the export of dual use technology. The EU Regulation (EC) No 428/2009 for the control of exports, transfer, brokering and transit of dual-use items is obviously also applicable in Finland.

10 France

Olivia Tambou (Paris-Dauphine University), Maitena Poelemans (CDRE, Universidad de Pau et des pauys de l'Adour)

10.1 Informed consent

10.1.1 General Regulatory Framework

Regulation	Type of regulation (hard law, soft law…)	Brief description and scope
Loi n°78-17 du 6 janvier 1978, (hereinafter LIL)	Main hard French Law on data protection which was modified by the loi n° 2018-493, 20 June 2018 and rewritten by the Ordonnance n°2018-1125 adopted on 12 December 2018 which came into effect on the 1st of June 2019.	**Art. 5 LIL** recalls that the consent is one of the legal grounds for lawful processing and refers to art. 4 §11 and 7 of GDPR. **Art. 45 LIL** is about the conditions applicable to the child's consent in application to art. 8 GDPR. (See section 3) **Art. 75 LIL** is the need in certain cases of an informed and "express" consent for health processing for scientific research purpose when the examination of genetics featured are necessary. Curiously, the GDPR term of explicit consent has not been used in French, which maintains the former used concept of "express consent" without a definition of it. **Art. 82** LIL transposed the consent of the e-privacy Directive. **Art. 85** LIL provides a specific consent of the data subject for the digital will. (See Section 4)
Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatiqu	Administrative Act considered as hard law The decree complete the LIL and also came into force on the 1st of June 2019	**Art. 114** lays down that the explicit consent according to art. 75 of the LIL must be written. When this is impossible, a third party, independent of the data controller must certify the express consent.