(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?

We are not aware that the Czech Science Foundation (https://gacr.cz/en/) or the Technology Agency of the Czech Republic (https://www.tacr.cz/en/homepage/) had taken any specific measures towards promoting of data protection in ICT R&I or facilitated the use of any particular instruments or DPIA methods. Both agencies issued statements about their compliance with the data protection framework, which however do not concern particularities of the supported instruments or tools (source: https://www.tacr.cz/dokums_raw/novinky/GDPR_souhrn.pdf (Czech) and https://gacr.cz/uredni-deska/ochrana-osobnich-udaju-a-gdpr-v-grantove-agenture-ceske-republiky/ (Czech).

(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?

Security research falls within the domain of the Ministry of Interior, which provides regulatory framework and relevant strategic plans and concepts (source: https://www.mvcr.cz/vyzkum/clanek/zakladni-informace-o-bezpecnostnim-vyzkumu-bezpecnostni-vyzkum.aspx (Czech)). We are not privy to the information regarding available tools to protect against industrial espionage and other confidentiality breaches for participating researchers and innovators. We are not aware of any publicly available information in this regard aside from aforementioned framework and strategic documents, which however do not contain any specific information on this topic.

On the other hand, customs Administration of The Czech Republic controls the export of dual use technology. This control generally does not prohibit or restrict the legal export of controlled technology, but individual deliveries are not allowed if there is a risk of abuse. It helps prevent possible damage to the political, security or business interests of the state, as well as prevent damage to the business interests of an entrepreneur, even by unintentional involvement in undesirable activities.

7 Denmark

Jesper Lund (IT-Political Association of Denmark), Sofie Flensburg (University of Copenhagen)

7.1 Informed consent

7.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope

Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN	Hard law	The main data protection framework implemented in Danish law in 2018
Databeskyttelses-loven (Danish Data Protection Act)	https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf (Unofficial English translation)	Hard law	Supplementary national provisions to the GDPR (GDPR implementation law)
Directive (EU) 2016/680 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN	Hard law	States the rules and requirements for data use and processing by authorities in connection with investigations and prosecution of criminal offences.

Lov om retshåndhævende myndigheders behandling af personoplysninger **(Law Enforcement Data Protection Act)**	https://www.retsinformation.dk/Forms/r0710.aspx?id=189891 (Danish)	Hard law	Processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Danish transposition of Directive (EU) 2016/680
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 the (Directive on privacy and electronic communications)	https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058	Hard law	Regulates the processing of personal data and the protection of privacy in the electronic communications sector
Bekendtgørelse om udbud af elektroniske kommunikations net og -tjenester **(Administrative Order for Provision of Electronic Communications Networks and Services)**	https://www.retsinformation.dk/forms/r0710.aspx?id=137773 (Danish)	Hard law	Contains the implementation of articles 6 and 9 of the ePrivacy Directive 2002/58/EU (data protection rules for traffic and location data in electronic communication services).
Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment (The cookie order)	https://danishbusinessauthority.dk/sites/default/files/cookie-exec-order-english-version.pdf	Hard law	Implements the ePrivacy Directive regulating the use of cookies for data collection and tracking
Act no. 128 on Electronic Communications	https://ens.dk/sites/ens.dk/files/Tele/act_on_elect	Hard law	Regulates data gathering and processing by suppliers of electronic

Networks and Services	ronic_communications_networks_and_services.pdf		communication services and public communication networks
Lov om TV-overvågning (Video Surveillance Act)	https://www.retsinformation.dk/forms/r0710.aspx?id=105112 (Danish)	Hard law	Data protection provisions for video surveillance (retention periods, rules for disclosure to third parties, and limits on where video surveillance may be performed)
Lov om videnskabsetisk behandling af sundheds-videnskabelige forskningsprojekter (Law on Scientific Ethical Treatment of Health Science Research Projects)	https://www.retsinformation.dk/Forms/r0710.aspx?id=192671 (Danish)	Hard law	Contains special provisions on the scope of informed consent in health science research projects
Seal for IT-security and responsible data use	https://via.ritzau.dk/pressemeddelelse/new-seal-for-it-security-and-responsible-data-use-is-in-its-way?publisherId=5540552&releaseId=13582237	Soft law	Official labelling scheme indicating that businesses carry out responsible cyber security and data use.

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

(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?

Processing of personal data that falls under the household exemption in the GDPR is also exempted from the Data Protection Act.

However, The Danish constitution and the Criminal Code both restrict individuals' access to obtain personal information about other individuals, pass it on, break the secrecy of post, telephony etc.

Section 264 d of the Danish Penal Code prohibits the disclosure of information or pictures about a person's private life. Section 264 b (a new provision, adopted in 2018)

prohibits using a GPS or similar device to register (track) someone's movements, unless the tracking is justified. It is possible that sections 264 b and 264 d of the Penal Code could apply in cases that would, in principle, fall under the household exemption 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)?

Data protection in connection with national security issues or investigations is regulated by the criminal code, the act on security of networks and information systems for operators of essential internet exchange points, the telecommunications act, and the Act on Processing of Personal Data by Law Enforcement Authorities

Section 3(2) of the Data Protection Act exempts the Danish Defence and Security Service (PET) and the Danish Defence Intelligence Service (DDIS) from the GDPR based on Article 2(2)(b) of the GDPR (national security). Both institutions are also exempted from the Law Enforcement Data Protection Act, transposing Directive (EU) 2016/680.

The national laws governing the operations of PET, DDIS and Centre for Cyber Security (CFCS, which is part of DDIS) contain their own specialised data protection provisions. These provisions are generally significantly weaker than the GDPR and Directive (EU) 2016/680 in terms of collection of personal data (e.g. requirements of a specific purpose), lawful processing, retention/erasure of personal data, and data subjects rights. In addition, the data protection rules in the DDIS law only apply to processing of personal data about Danish citizens and permanent residents, not foreign citizens residing outside Denmark.

Danish Security and Intelligence Service (PET) Law

https://www.retsinformation.dk/Forms/r0710.aspx?id=186190 (Danish)

Danish Defence Intelligence Service (DDIS) Law https://www.retsinformation.dk/Forms/r0710.aspx?id=193864 (Danish)

Centre for Cyber Security (CFCS) Law

https://www.retsinformation.dk/Forms/R0710.aspx?id=209851 (Danish)

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
The Danish Data Protection Agency	https://www.datatilsynet.dk/english/	Yes	About 60 employees (end of 2018)	Average, with a focus on legal compliance with the GDPR and the Data Protection Act, as well as providing general guidance to controllers	According to the DPA's annual report for 2018, responding to questions from the public is a priority. The DPA has published several recommendations and opinions (not

					related to specific complaint cases) on its website.
The Court Administration (Domstolsstyrelsen) **(Supervisory authority for processing of personal data carried out for the courts when they do not act in their capacity of courts)**	http://www.domstol.dk/om/otherlanguages/english/thedanishjudicialsystem/courtadministration/Pages/default.aspx	Yes	Unknown (shared with other tasks of the Court Administration)	Low (due to the limited scope of this supervisory authority)	No (not relevant for this supervisory authority)
The Danish Business Authority	https://danishbusinessauthority.dk/	Yes	Approximately 650 that deal with all types of business-related issues (including supervision of the cookie rules and telecommunications regulation)	According to the information on the Business Authority's website, only one ruling has been made on the basis of the cookie order, while the authority received 1131 reports on data security breaches in 2018. This indicates that the telecommunications sector as well as the regulators have strengthened their attention to	The Danish Business Authority is mainly aimed at businesses and advise on the use of cookies and security issues for telecommunications companies. However, the authority also provides information on how to block and delete cookies. The public can call or write the authority.

				data security since the introduction of GDPR.	

Information regarding Data Protection Authorities, Denmark

(i) 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.?

Section 10(1) of the Data Protection Act provides that personal data mentioned in GDPR Article 9(1) (sensitive personal data) and Article 10 (criminal convictions and offences) may be processed for the sole purpose of carrying out statistical or scientific studies of significant importance to society if the processing is necessary in order to carry out such studies.

Section 10(1) provides a legal basis for processing sensitive personal data without consent of the data subject in research projects of significant importance to society, assuming that research is the sole purpose of the processing. The concept of "significant importance to society" is not defined in legislation, but follows administrative practice. The threshold is generally believed to be quite low, even though "significant" is part of the requirement.

Apart from the definition of scientific studies of significant importance to society, there is no special definition of data processing for research purposes in Danish legislation.

(ii) 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?

The legal basis for processing sensitive personal data for research purposes in Section 10(1) of the Data Protection Act implements Article 9(2)(j) and Article 89 of the GDPR. This Act §10 allow processing of sensitive personal data without consent of the data subject, if the processing is carried out solely for the purpose of statistical or scientific studies of significant societal value. The same applies to ordinary personal data. The data processing must be necessary for conducting the studies and the data cannot be used for e.g. journalistic purposes, administration, or treatment of patients. The data can be used in anonymized form for other purposes and the final results can be disseminated in public if the individual data subjects cannot be identified.

The following safeguards for research processing are specified in Section 10 of the Data Protection Act:

- The personal data may not be processed for other purposes than scientific (research) and statistical purposes.
- Disclosure of the data to a third party requires prior DPA approval if the third party is outside the EU/EEA, if the disclosed personal data relates to biological material, or if the disclosure is made for the purpose of publication in a recognised scientific journal or similar.
- The DPA may lay down general conditions for disclosure, including but not limited to disclosure that requires prior authorisation. An example of a general condition for disclosure of personal data processed for research purposes could be the use of pseudonymisation.

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

Danish legislation generally follows GDPR with regards to protection of sensitive data.

Apart from distinguishing between non-sensitive and sensitive data, Danish legislation (the Criminal Code and the Public Administration Act) includes a third category of 'confidential information' covering e.g. social security numbers, personal finances, education, working, employment, family affairs etc. that are not necessarily sensitive but should not be available for the general public.

Section 7 of the Data Protection Act allows processing of sensitive personal data with appropriate safeguards in the following cases:

- If the conditions laid down in points (a), (c), (d), (e) or (f) of GDPR Article 9(2) have been complied with. No specific safeguards are required in these cases.
- If the processing is necessary for the purposes of meeting and respecting the data controller's or the data subject's labour law obligations and specific rights, in accordance with point (b) of GDPR Article 9(2). No specific safeguards are required in this case.
- If the processing is necessary for preventive or occupational medicine in accordance with point (h) of the GDPR. The required safeguard is that the processing may only be performed by health professionals subject under law to the obligation of professional secrecy in the Danish Health Act (sundhedsloven).
- If the processing is necessary for reasons of substantial public interest. This is a general implementation of GDPR Article 9(2)(g), covering all types of sensitive personal data. For public controllers, no specific safeguards are required. Private controllers must obtain prior DPA authorisation, and the DPA may lay down further conditions for processing. This provision was recently used to give DPA authorisation for automated facial recognition at a football stadium.
- In other cases ("catch all" provision), competent ministers in consultation with the Minister of Justice (who is responsible for data protection) may lay down more detailed ruled regarding the processing of sensitive personal data. This power has not been used yet.

Furthermore, Section 12 of the Danish Data Protection Act allows processing of personal data covered by Article 9(1) in an employment relationship if the processing is necessary for the purpose of observing and respecting the employment law obligations and rights of the controller or of the data subject as laid down by other law or collective agreements.

The exemptions and derogations for freedom of expression and journalistic purposes in the Data Protection Act (in accordance with GDPR Article 85) also cover sensitive personal data [GDPR Article 9(1)].

(iv) 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.)?

The Danish Ministry of Higher Education and Science has published a Danish Code of Conduct for Research Integrity that provides a framework for conducting responsible research and includes guidelines and rules for the management of data. The code is not legally binding in itself, but all Danish universities have registered as adhering to it. The code encourages research institutions to further develop policies and procedures for

research integrity and states that research institutions should have a policy on safe storage, disposal and retention of data and provide secure data storage facilities "that are consistent with confidentiality requirements and applicable regulations and guidelines, e.g. on the processing of personal data". It also states that institutions should "allow access to the stored primary materials and data, except when this is in conflict with contractual legal obligations or current regulations on for example ethical, confidentiality or privacy matters or intellectual property rights". Denmark also has a health research ethics committee system consisting of a national committee and 12 regional committees that must be notified of research projects that involve human biological material. The rules for using this type of data with or without informed consent is stated in the Act on Research Ethics Review of Health Research Projects. For instance, if data subjects are unable to give informed consent, data obtained from these individuals can be used if the project is likely to directly improve the life and condition of these patients or patient groups. The Danish Health Care Act and the Medicine Act also include rules on the disclosure of individuals' health information.

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

The definition of data processing for statistical purposes has the same scope as processing for scientific studies (research). Section 10 of the Data Protection Act covers statistical and research purposes with the same provisions and safeguards.

(vi) 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.)

Requirements for appointing a DPO and performing a DPIA follow the GDPR, and there are no special requirements for research projects in Danish legislation. In this sense, all Danish Universities are required to have a DPO. A DPIA is to be performed when new technologies are used for data processing, if there is a high risk of violating the data subjects' rights, or if the data processing can have significant repercussions for the participants.

The duty to collect consent in health science research projects involving human biological material is partially regulated by the Law on Scientific Ethical Treatment of Health Science Research Projects. See the answer to the previous question.

7.1.2 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.)

Legal persons are data subjects in certain cases. This applies to processing of data by credit information agencies and disclosure to credit information agencies of data on debt owed to public authorities. Government ministers may lay down further rules extending the Data Protection Act to include legal persons.

At same time, The Danish Data Protection Act includes various specifications on the use of data in connection with employment. An employer is, as a rule, allowed to process an employee's personal data in connection with the employer's HR administration without obtaining employee consent or authorization from the Data Protection Agency. This type of processing must be justified for operational reasons and may not be offensive to the

employee. The controller must also inform the employee of the processing no later than six weeks before.

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

The Data Protection Act does not contain any special requirements (relative to GDPR Article 7) regarding what constitutes informed consent.

The Data Protection Act requires consent for certain types of processing, e.g. for disclosure of personal data to another company for the purpose of direct marketing and for processing of the national identification number by private entities, unless the processing of the national identification number is required by law (e.g. for tax reporting purposes).

The Data Protection Act provides that sensitive personal data (GDPR Article 9) and criminal offences (GDPR Article 10) can be processed with explicit consent of the data subject. In certain situations, defined in the Act, disclosure or processing can be done without the consent of the data subject.

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

Data processing for specific purposes (e.g. research, statistics, investigations, health research etc.) described above.

The Data Protection Act contains special provisions adapting the GDPR for these cases of data processing:

- Disclosure of personal data to another company for the purpose of direct marketing can only be done with consent of the data subject, as the general rule (section 14 of the Data Protection Act). Only general data that forms the basis for classification into customer categories can be disclosed based on a legitimate interest.

- Data processing by credit information agencies is subject to a detailed regulation in parts 4 and 5 of the Data Protection Act. It is regulated in a detailed manner when information about overdue debt may be disclosed to a credit information agency and when this information must be deleted by the credit information agency. The special rules on credit information agencies also apply to credit information about legal persons.

In addition, the Video Surveillance Act contains provisions regarding areas where video surveillance is banned for private entities. In practice, these provisions are interpreted as allowing video surveillance in public areas where it is not banned. The maximum retention period for video recordings, and rules on disclosure of recordings to third parties, are also regulated by the Video Surveillance Act.

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

There are no special requirements for exercising data subjects rights. However, Danish national law contains a number of restrictions of these rights under the GDPR and the Law Enforcement Data Protection Act. For PET and DDIS (national security area), all data subjects rights can only be exercised indirectly through the Intelligence Oversight Board (supervisory authority). Upon request from a citizen, the Intelligence Oversight Board will check whether personal data about the citizen is processed lawfully.

Data subjects can complain first to the data controller and secondly to the Data Protection Agency or the courts if the controller refuses to handle the complaint. Data controllers must reply immediately or within a month after receiving the request unless the issue is highly complicated, while the Data Protection Agency must reply within three months. The Act on Processing of Personal Data by Law Enforcement Authorities also states that data subjects have the right to have information rectified, completed, deleted etc. in case the information is incorrect or incomplete.

7.1.3 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)?

As the public sector is highly digitized in Denmark, various acts and strategies regulating e.g. the health sector, criminal enforcement, social security, education etc. now include specialized rules on the processing and exchange of personal data in these particular sectors. These all built on the general Danish data protection legislation and GDPR.

The special rules in the Data Protection Act about credit information agencies, as well as rules about processing for the purpose of warning others against having a business relationship with or accepting employment with a data subject ("warning lists"), apply to data about legal persons as well.

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

Children are subject to specific protection especially with regard to use of personal information for marketing purposes, for personality or user profiles and when they use services that are aimed directly at children. Children can provide consent for Information Society services such as social media from the age of 13, while other types of services require an individual assessment. As a general rule, the Danish Data Protection Agency states that children older than 15 can provide consent.

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

Not in the data protection act as such, but the Data Protection Agency has published various guides, that extend the definition of vulnerable individuals to mentally ill persons, asylum seekers, etc. Employees are also considered as vulnerable when they are asked for consent by their employers.

7.1.4 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 Danish Data Protection Act and the General Data Protection Regulation apply to the data of deceased persons for a period of 10 years following the death of the deceased. However, there are no specific rules on how data about deceased individuals can be processed or on whether or not close relatives can provide consent on behalf of the deceased or ask for data to be deleted.

Special data protection provisions regarding deceased persons in other laws, e.g. the Health Act (sundhedsloven), take precedence over the 10-year rule.

The Minister of Justice may lay down rules in specific cases with a shorter or longer protection period for deceased persons than 10 years. This power has not been used yet.

7.1.5 Accountability and Data Protection Impact Assessment

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

The Data Protection Act does not contain any further provisions (in addition to those of the GDPR) related to general accountability.

In 2019, the Danish Minister for Industry, Business and Financial Affairs launched a prototype of a labelling system for IT-security and responsible data use that will be implemented in 2020. The goal is to make consumers feel safe and comfortable with the way companies are handling their personal data and to make it easier for consumers to actively choose companies with a responsible behaviour in terms of data ethics. The labelling system is developed in cooperation with industry stakeholders and companies register voluntarily.

(iv) 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?

Carrying out a DPIA is mandatory when the data processing is "likely to result in a high risk to the rights and freedoms of natural persons" (cf. GDPR Article 35 (1)). The Danish Data Protection Agency has published a guide specifying that DPIAs should be conducted when introducing new technologies or using existing technologies in new ways and the personal and social consequences are unknown. It also specifies the definition of 'high risk to the rights and freedoms of natural persons' as data processing that can inflict physical, material, or immaterial harm – more specifically, discrimination, identity theft, financial losses, lost control over personal and sensitive information etc. When performing a DPIA, the Data Protection Agency notes that four steps should be taken: First, is should be assessed if the given data processing entails a high risk to the rights and freedoms of natural persons; secondly, the impact assessment should be performed; on the basis of which appropriate measures to limit the identified risks should be taken; if it is impossible to limit the risks, the Data Protection Agency should be notified before starting the processing. The guide also includes specific questions that should be answered when conducting a DPIA.

7.2 Commercialization of data

7.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Basic Data Program	http://grunddata.dk/english/	Administrative practice	Denmark has a number of central registries with information about persons (Civil Registration System),

(Agency for Digitalisation - Ministry of Finance)	https://datafordeler.dk/dataoversigt/		companies (Central Business Register), properties (Building and Dwelling Register), and geographical information (maps, street addresses). The purpose of the Basic Data Program is to make some of this data accessible to public authorities and private companies through the "Data Distributor" (Datafordeleren). A number of online services have been developed based on personal data and other data from the Basic Data Program and the Datahub (see below).
Datahub **(Danish Business Authority - Ministry of Industry, Business and Financial Affairs)**	http://datahub.virk.dk/publisher/erhvervsstyrelsen Central Business Register Act https://www.retsinformation.dk/Forms/R0710.aspx?id=210014 (Danish)	Administrative practice and hard law	Public access to company registration data in the Central Business Register (CVR). Section 18 of the Central Business Register Act grants public access to information about company registrations, including owners, with some exceptions.
Civil Registration Act (CPR-loven)	https://www.retsinformation.dk/Forms/R0710.aspx?id=191719 (Danish)	Hard law	One of the purposes of the Civil Registration Act is to make information about names and addresses available to private companies that have a legitimate interest in the information.
Act on Electronic Communications Networks and Services **(Teleloven)**	https://ens.dk/sites/ens.dk/files/Tele/act_on_electronic_communications_networks_and_services.pdf (unofficial English translation)	Hard law	Section 31 of the Act on Electronic Communications Networks and Services requires that providers make subscriber information (telephone number, name and address) available to all parties who wish to receive the data, unless the subscriber has explicitly opted out of this data sharing. The main intended recipients of the subscriber information are providers of public telephone directories, in

			accordance with Article 12 of the ePrivacy Directive 2002/58. However, the data is also acquired by companies that combine ("enrich") the telephone subscriber information with other information for various purposes of data commercialisation (e.g. big data, direct marketing and market segmentation analysis).
The Marketing Practices Act	https://www.consumerombudsman.dk/media/14553/markedsforingsloven-lbkg-2013.pdf	Hard law	Regulates business activities online and off including the collection, use and redistribution of contact information for marketing purposes.
The cookie order	https://danishbusinessauthority.dk/sites/default/files/cookie-exec-order-english-version.pdf	Hard law	Implements the ePrivacy Directive. Regulates the use of cookies for data collection and tracking

Main regulatory tools addressing data commercialization in Denmark.

7.2.2 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. Danish law does not have any general restrictions on exchanging personal data for services, for example access to an app. The main protection of the consumer will be the GDPR, for example the possibility to withdraw consent and the right to erasure.

Danish law has a general principle of freedom of contract which also applies to contracts with consumers. However, Section 36 of the Danish Law on Contracts provides that a contract can be changed or set aside, in whole or in part, if the contract terms are unreasonable to one of the parties. The threshold for this is lower in consumer contracts if there is an imbalance in the rights and obligations of the parties (the business and the consumer). It is possible that this provision related to unfair contractual terms could affect certain contracts based on exchange of personal data for access to a service.

In very specific cases, companies are prohibited from receiving certain types of personal data, even with the explicit consent of the data subject. Insurance companies are not allowed to receive genetic information (e.g. DNA analysis) that may reveal predisposition to diseases about their customers.

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

Online services in the area of electronic communication (email, chat) and social media are frequently provided to online users in exchange for personal data. The situation in Denmark is similar to the rest of the European Union.

Many online and physical stores have customer loyalty programs, where information about purchase behaviour is provided (allowed to be processed) in exchange for discounts or access to other special benefits for consumers.

Car insurance companies regularly offer discounts on the insurance premium if the insurance customer provides information about his/her driving behaviour, typically through a data collection device ("black box") installed in the car.

(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 Danish regulation requiring renumeration of data subjects if profit is made out of their personal data.

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

The Data Protection Act has exemptions and derogations from the GDPR that allow secondary use of personal data for archival, statistical and scientific research purposes.

The Central Business Register Act creates a general public access right to data about business registrations, with some opt-out exceptions. In effect, this allows secondary use of business registration data, e.g. for marketing and business analytics purposes.

The Act on Electronic Communications Networks and Services allows secondary use of telephone subscriber information since providers of electronic communication services are required to disclose the data to anyone who wish to receive it (and is willing to pay the marginal cost of providing the data). There is no effective purpose limitation for the disclosed subscriber data, so secondary use is allowed.

Secondary use is also possible in other cases, where personal data is made available to the public or companies, either through administrative practice or legal provisions.

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

Metadata that is not personal data, as well as non-personal data (including personal data that is made truly anonymous), falls outside the scope of the Data Protection Act (as well as the GDPR).

Information that is not personal data can be legally protected as business secrets. Collection of information (databases) may be protected, even if the individual pieces of information are not protected, see the answer below.

Telecommunications operators are prohibited from saving and processing traffic and localizing data that is not necessary for the functionality of the electronic communication service unless the data is anonymized or the customer provides consent.

7.2.3 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?

The Danish government has an ongoing strategy for "digital growth" (link to English version: https://eng.em.dk/media/10566/digital-growth-strategy-report_uk_web-2.pdf), where data, including personal data, plays a pivotal role and described as the "driver of growth in trade and industry". The focus is on making non-personal as well as personal data available and creating new business opportunities based on data. This corresponds

to seeing data, including personal data, as a primary commodity (raw material) similar to oil.

(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 copyrighted works is protected under the Danish Copyright Act, in accordance with the EU Infosoc Directive. The Sui Generic protection in the EU Database Directive 96/9/EC is also implemented in the Danish Copyright Act.

The Danish Marketing Act has a general clause (Section 3) that requires proper marketing practices ("god markedsføringsskik") vis-à-vis consumers, other businesses and public interests of society. This general clause may provide some protection against commercial exploitation of data by other companies, including freely available online information that is harvested through web crawling. For example, an injunction against an online news indexing service was based on the general clause in the Marketing Act in combination with the sui generis database protection right (Newsbooster, case U 2003.1063 SH).

We are not aware of any mechanisms in Danish (case) law to determine the value of data.

7.3 Security and cybersecurity

7.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Guidance on security of processing and data protection by design and by default, June 2018 **(Danish Data Protection Agency, Ministry of Justice and Agency for Digitalisation)**	https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf (in Danish)	Guidance (soft law)	Before the GDPR, there was a binding security code ("sikkerhedsbekendtgørelsen") for public controllers. Since GDPR Article 32 relies on a risk-based approach, the security code has been replaced by this guidance. Apart from this guidance (which is not legally binding), the security provision in the GDPR is not reflected in Danish regulation.
Law Enforcement Data Protection Act	https://www.retsinformation.dk/Forms/r0710.aspx?id=189891 (Danish)	Hard law	Contains security requirements for law enforcement, in accordance with Directive (EU) 2016/680
Security regulations for the Danish	PET https://www.retsinformation.dk/For	Hard law	Requires PET and DDIS to implement appropriate technical and organisational measures to

Security and Intelligence Service (PET) and the Danish Defence Intelligence Service (DDIS)	ms/R0710.aspx?id=201486 (Danish) DDIS https://www.retsinformation.dk/Forms/R0710.aspx?id=202374 (Danish)		protect personal data. The regulation for PET is more detailed than the one for DDIS.
Lov om Center for Cybersikkerhed **(Centre for Cyber Security Act)**	https://www.retsinformation.dk/Forms/R0710.aspx?id=209851 (Danish)	Hard law	Main law establishing the Centre for Cyber Security (CFCS) as part of the Danish Defence and Intelligence Service (DDIS). The law authorises CFCS to collect, retain and analyse network traffic (content as well as metadata) from institutions that are monitored by CFCS for the purpose of preventing and investigating cyber security incidents. Public authorities and private companies can, upon request, be monitored by CFCS. The monitoring of network traffic and processing of personal data by CFCS is exempted from the GDPR based on the national security exemption (as CFCS is part of DDIS). In cases of critical infrastructure, CFCS can demand that the network traffic of a public authority or private company is subjected to monitoring by CFCS.
Lov om net- og informationssikkerhed **(Network and Information Security Act)**	https://www.retsinformation.dk/forms/r0710.aspx?id=176300 (Danish)	Hard law	Cyber security requirements for providers of electronic communications networks and services. The Centre for Cybersecurity (CFCS) is the supervisory authority. The law implements the security and integrity requirements in the

			Framework Directive 2002/21/EC. CFCS can issue orders that require providers of publicly available electronic communications networks and services to implement specific measures in order to ensure the information security. Providers are required to notify CFCS before signing agreements with vendors of equipment and services. CFCS may require a standstill period of 10 business days for consultation with CFCS before an agreement with a vendor can be signed.
Implementation of the NIS Directive **(sector-specific laws)**	**Health sector** https://www.retsinformation.dk/Forms/R0710.aspx?id=201048 (Danish) **Transport** https://www.retsinformation.dk/Forms/R0710.aspx?id=201058 (Danish) **Digital infrastructure** DNS and TLD https://www.retsinformation.dk/Forms/r0710.aspx?id=201060 (Danish) IXP https://www.retsinformation.dk/Forms/R0710.aspx?id=201052 (Danish) **Banking and financial market infrastructure** Sections 307 a, 354(6) and 354 h	Hard law	The NIS Directive is implemented a through a number of sector-specific laws or amendments to existing laws. CFCS is the single point of contact (cf. Article 8(3) of the NIS Directive) and the only Danish CSIRT (cf. Article 9(1) of the NIS Directive). Competent authorities (cf. Article 8(1) of the NIS Directive) are existing authorities in each sector with no special expertise in cybersecurity matters.

	of the Financial Services Act https://www.retsinformation.dk/Forms/R0710.aspx?id=209982 (Danish)		

Main regulatory tools addressing security and cybersecurity in Denmark

7.3.2 Implementation of EU Law

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

Under the GDPR, there are no particular procedures for security measures in Danish law based on EU law, only a guidance for controllers (see above).

The Danish law transposing the Law Enforcement Data Protection Directive 2016/680 has provisions on security of processing that closely follow the Directive. The Minister of Justice can demand that certain databases are located in Denmark (data localisation requirement).

Public authorities are required to follow the ISO 27001 standard for management of information security systems and the Data Protection Agency's guidelines state that it is mandatory to use encryption when transmitting confidential and sensitive personal data by email via the internet. The Danish Data Protection Agency has not set up specific requirements to the type of encryption that should be used, except that the level of encryption should be appropriate relative to the risk.

(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 fully implemented in Danish law.

This was done through a number of sector-specific laws and, in some cases, amendments to existing laws. See the table above.

The Centre for Cybersecurity (CFCS) is the single point of contact (defined in Article 8(3) of the NIS Directive) and the only Danish CSIRT (defined in Article 9(1) of the NIS Directive). Competent authorities are existing (supervisory) authorities in each sector. In most cases, the designated supervisory authorities had limited experience in cybersecurity matters prior to becoming a competent authority under the NIS Directive.

The Danish government has adopted a national strategy on the security of network and information systems, as required by Article 7 of the NIS Directive. Link to English version:
https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf

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

The Data Protection Agency provides various guidelines for the protection of personal data and advises organizations on how to e.g. carry out DPIAs. Public institutions are, as mentioned above, required to follow the ISO 27001 standard and The Government IT Council has established a Government Information Security Forum (GISF), in which about 30 government institutions participate. The Forum exchanges experiences with the

use of the ISO 27001 standard, follows the general development of information security management and proposes initiatives to increase information security.

7.3.3 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?

Under the Danish implementation of the NIS Directive, operators of essential services are required to notify the competent authority and the Centre for Cyber Security (as CSIRT) of incidents which have a significant impact on the continuity of the service provided. This follows Article 14(3) of the NIS Directive.

Providers of public electronic communications services are required to notify the Danish Business Authority of personal data breaches. If the incident involves a particular risk for the security of personal data, the subscribers must also be notified. These requirements are specified in the Act on Electronic Communications Networks and Services (transposing Article 4 of the ePrivacy Directive 2002/58 for the personal data breaches).

Providers of public electronic communications networks and services are also required to notify the Centre for Cyber Security (CFCS) of information security breaches which have a significant impact on the continuity of the service. This requirement is specified in the Network and Information Security Act.

7.3.4 Supervision of cybersecurity

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

The NIS Directive Article 14(2) grants competent authorities certain limited enforcement power to demand information from operators of essential services about security policies. These powers are implemented in Danish law.

For providers of public communications networks and services, the Network and Information Security Act grants additional enforcement powers to the Centre for Cyber Security (CFCS). CFCS can issue orders that require providers to implement specific measures in order to ensure the information security of their networks and services. Providers are required to notify CFCS before signing agreements with vendors of equipment and services. CFCS may require a standstill period of 10 business days for consultation with CFCS before an agreement with a vendor can be signed.

For critical infrastructure, CFCS has enforcement powers under the Centre for Cyber Security Act. CFCS has powers to monitor network traffic (content and metadata) and stationary data (data stored on servers, computers and mobile devices) if the public authority or company has requested such monitoring from CFCS. If the public authority or private company represents a particular importance to society, CFCS can decide that the network traffic must be monitored by CFCS.

CFCS has enforcement powers to block network traffic if there is a substantiated suspicion of a cybersecurity incident. Blocking network traffic requires the consent of the public authority or private company whose network traffic is monitored. With prior court approval, CFCS can issue production orders to service providers for information about the user of an email address, IP address or domain name.

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

The Centre for Cyber Security (CFCS) is responsible for preventive national advisory and information activities associated with cyber security in both the public and the private sector.

Danish cybersecurity regulation, described above, gives CFCS additional competences and responsibilities in specific areas. CFCS is the single point of contact and the CSIRT in the Danish implementation of the NIS Directive. For providers of public communications networks and services, CFCS has detailed supervisory powers to ensure a high level of information security.

For public authorities and private companies that represent critical infrastructure, CFCS has powers to monitor network traffic for the purpose of preventing and investigating cybersecurity incidents if requested by the public authority or private company. In certain cases, CFCS can demand that the network traffic is monitored by CFCS.

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

Breaches of data and cybersecurity can be reported to the Data Protection Agency, the Centre for Cyber Security and the police. This division of responsibilities has been criticised since it is unclear when a breach should be reported to one authority as opposed to another. The Data Protection Act states that data subjects can be compensated for all types of material and immaterial harm due to illegal data processing including disclosure of personal information.

Damages for lack of cybersecurity would follow the general principles of claims for compensation in Danish (case) law. There is no specific regulation for cases involving lack of cybersecurity. In general, liability requires some negligent behaviour (the culpa rule) and a connection between the negligent behaviour and the monetary loss (damages) for which compensation is claimed.

If a person is affected by the lack of cybersecurity, the liable part can be ordered to pay compensation for tort. This can be relevant in data breach cases.

7.4 Enforcement: fines and sanctions

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

Under section 41 of the Data Protection Act, violations of the GDPR and the Data Protection Act can be punished with fines or prison sentences up to 6 months, unless a higher punishment follows from other legislation. When determining the level of fines, GDPR Article 83(2) must be adhered to. Due to the legal system in Denmark, all GDPR fines will be a criminal penalty rather than an administrative fine.

Chapter 27 of the Danish Penal Code, "Offences against Personal Honour and Certain Individual Rights", contains various provisions that involve processing personal data.

Section 264 d prohibits the disclosure of information or pictures about a person's private life. Violations are punished by fines or prison up to 6 months, which can increase to three years in severe case.

Section 264 b (a new provision, adopted in 2018) prohibits using a GPS or similar device to register (track) someone's movements, unless the tracking/surveillance is justified. It is not a condition for applying section 264 b that the processing infringes data subject rights under the GDPR. Violations can be punished by fines or prison up to 6 months.

Violations of the Danish cybersecurity laws (see above) can be punished with fines.

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

The Danish Constitution does not allow administrative fines. Only courts can issue fines in Denmark. This is reflected in recital 151 of the GDPR which provides that in Denmark, fines will be imposed by competent national courts as a criminal penalty.

If the sanction for the violation of the GDPR or the Data Protection Act only involves a fine, the Data Protection Agency can propose a fine to the offending party. If the offending party does not accept the (proposed) fine, or if the sanction for the violation may involve a prison sentence, criminal prosecution is necessary so that a court can issue the fine as a criminal penalty for the data protection offence. In these cases, the Data Protection Agency will refer the case to the Danish Police.

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

Data protection offences under the Data Protection Act can be sanctioned at the initiative of the Data Protection Agency ("own initiative" case). A complaint from the injured party is not required.

Offences under chapter 27 of the Danish Penal Code are primarily subject to private prosecution, which means that the injured party must litigate the (criminal) case in court. However, there are exceptions to this, especially for section 264 d, where the injured party can request public prosecution.

7.5 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?

The Law on Scientific Ethical Treatment of Health Science Research Projects requires approval by a scientific ethical committee if the research project involves biological material. The approval must be obtained by the researcher before the research project starts.

There is no requirement for prior approval by an ethical committee if the research project only uses personal data from existing health databases.

Apart from these cases of data-based health science research involving biological material, there is no legal requirement for review of data protection issues in research projects. However, some faculties and departments at Danish universities have established voluntary ethics committees.

The University of Southern Denmark has a Research Ethics Committee, which is a non-compulsory offer to researchers https://www.sdu.dk/en/forskning/service_til_forskere/forskerstoette/ansvarlig+forsknings praksis/research+ethics+committee (description in English)

The Research Ethics Committee can consider data protection issues. Research projects in social sciences based on Danish registries (public databases) without consent of the data subject are specifically mentioned as something that the committee can consider.

University of Aarhus and University of Copenhagen have research ethics committees that can provide an assessment of a research project if this is required by the research funding agency.

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

The publicly financed Independent Research Fund in Denmark explicitly requires projects to adhere to the Danish Code of Conduct for Research Integrity, which as described earlier recommends that research institutions follow various guidelines when using personal data. A wide range of other funding institutions have also signed this, but do not explicitly require research projects to follow these guidelines and none of the largest private foundations for research in Denmark require any ethical self-assessment, reviews etc. at the proposal state or explicitly mentions data protection in their funding policy or their guidelines for applications.

The guidance for research projects by the Danish Data Protection Agency mentions that unauthorised access to the personal data must be prevented, that the personal data should be protected against destruction, loss or alteration, and that processing of personal data must not exceed what is necessary for the purpose. The controller is also required to assess the risk for the data subject. Everything in the guidance for research project (link: https://www.datatilsynet.dk/emner/forskning-og-statistik/generelt-om-forskning-og-statistik/) seems to be general GDPR-related guidance, not specifically related to processing personal data for research projects.

Pseudonymisation is commonly used in registry research projects. The national identification number (CPR-number) is used to combine different registries and is then replaced by a pseudonymous identifier in the data set used for research. The national identification number may still be kept by the researcher (separately), for example for combining the research data with new information in the future.

(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?

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