research, they contain important information applicable to research. AEPD has also produced a "Code of good practice on data protection for Big Data projects" https://www.aepd.es/es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (Spanish).

(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?

As far as we are concern there are not specific regulation or procedure for ICT R&I involving defence, dual use of technology or affected by embargoes. In terms of regulation there exist a specific framework for dual use technology trade, established in the Law 53/2007 of 28 December 2007 on the control of foreign trade in defence and dual-use material and the related Royal Decree 679/2014, of 1 August, approving the Regulation on the control of foreign trade in defence material, other material and dual-use products and technologies. Nonetheless this regulation does not directly affect R&I.

On the other hand, there are concrete program for promoting research of Centre for the Development of Industrial Technology (Centro para el Desarrollo Tecnológico Industrial (CDTI)). CDTI is a Public Business Entity, under the Ministry of Science and Innovation, which promotes innovation and technological development of Spanish companies. It is the entity that channels applications for aid and support for R&D&I projects from Spanish companies at national and international level. A Collaboration Protocol has recently been signed between the Ministry of Defence and the Ministry of Science and Innovation involving the CDTI, in which the parties undertake to exchange information and act in coordination to support R&D&I in the defence sector.

The CDTI has created a specific department for Large Installations and Dual Programmes to directly attend to the needs of the defence and security sector in terms of business R&D&I, with tasks of promotion, management, representation, advice and strategic evaluation.

27 Sweden

Patricia Jonason, Anders Wainikka (University of Södertörn)

27.1 Informed consent

27.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope

Regeringsformen **The Instrument of Government**	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kungorelse-1974152-om-beslutad-ny-regeringsform_sfs-1974-152 (Swedish)	Hard law (Constitutional law)	Enshrines the right to the protection against "*significant infringments* [made by the State] *in the individuals privacy if it occurs without consent and consists in surveillance or the mapping of the personal circumstances of the individual*". (Chapter 2, Section 6)
Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ***Act (2018:218) with supplementing provisions to the EU Data Protection Regulation*** **(in short, the Data Protection Act (DPA)**		Hard law	Supplements the GDPR with provisions on the legal basis for the processing, on the processing of certain categories of personal data, on limitations of use related to archives and statistics, on limitations of certain rights and obligations, on the supervisory authority's handling and decisions and on damages and appeal.
Förordning (2018:219) med kompletterande bestämmelser till EU:s	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218	Hard law	Contains inter alia provisions of organizational character, such as the designation of

dataskyddsförordning **Ordinance (2018:219) with supplementing provisions to the EU Data Protection Regulation** **(in short, the Data Protection Ordinance (DPO)**	(Swedish) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219 (Swedish)		the Data Protection Board and of the accreditation body and the enforcement of decision on fees (sanktionsavgifter)
Brottsdatalag (2018:1177) ***Criminal Data Act (2018:1177)***	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177 (Swedish)	Hard law	Special regulation for some authorities which have the task of combatting crime
Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område ***Swedish Act (2018:1693) on processing of personal data by the police***	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693 (Swedish)	Hard law	Regulates the use of personal data for police purposes
Lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20191182-om-sakerhetspolisens-behandling_sfs-2019-1182 (Swedish)	Hard law	Regulates the use of personal data for the security service

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

(ix) 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?

No

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

The point of departure is that the scope of application of the general rules of the data protection legislation goes beyond the requirements of the GDPR and encompasses even the "processing of personal data in the course of an activity which falls outside the scope of EU law" (DPA, Chap. 1, Section 2).

However, exemptions are made in the field of national security. Neither the GDPR, nor the DPA apply to activities covered by:

1. the Act (2007:258) concerning the Processing of Personal Data in the Armed Forces Defence Intelligence and Military Security Service (Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst).

2. the Act (2007:259) on Processing of Personal Records within the Scope of the Defence Intelligence and Development Activities of the National Defence Radio Establishment (Lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet)

3. the Act (2019:1182) Concerning the Swedish Security Service's Processing of Personal Data (Lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter).

Name of Authority	Link (English version if possible be)	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
Datainspektionen (DI)	https://www.datainspektionen.se/other-lang/	yes	About 95	Intermediate	The DI has an efficient hotline service. However, it can take weeks or months to receive a response to questions sent by email.

Information regarding Data Protection Authority

(xi) 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.?

The Swedish legislation does not provide for a definition of "data processing for research purposes", nor for "research in public interest". However, the Act (2003:460) concerning the Ethical Review of Research Involving Humans, the Ethical Review Act (lag (2003:460) om etikprövning av forskning som avser människor) defines research as : "Scientifically experimental, theoretical work or scientific studies, when the work or the studies are carried out for gathering new knowledge and development outcomes on a scientific basis, excluding work or studies that are performed solely within the framework of higher education on the basic or advanced level".

(xii) 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 main safeguard consists in the ethical review, carried out by an Ethical Review Authority (Etikprövningsmyndigheten), that research projects which involve the processing of sensitive data and data on criminal offences have to undergo before the research is able to start [more details on the ethical review are provided under Part 5].

No reference to the ethical review procedure is made in the DPA on the contrary to what was the case with the precedent Swedish Data Protection regulation, the Personal Data Act (personuppgiftslagen 1998:204).

However, a Research Data Act, that has been drafted but not yet adopted, contains a provision according to which sensitive personal data and data on criminal offences may be processed if the processing is deemed necessary for research purposes and if it has been approved according to the Ethical Review Act.

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

Among the specific safeguards the following examples can be mentioned:

The requirement of ethical review when it concerns research, according to the Ethical Review Act.

The prohibition to conduct searches based on sensitive personal data for the purpose of obtaining a selection of persons in cases of processing of sensitive data by a public authority when the data have been provided to the authority and the processing is required by law (DPA, Chap. 3, Section 3).

The requirement of the Swedish Data Protection Authority's consent for the processing of personal data other than health data in quality registers. (Patient Data Act, (Patientdatalagen (2008:355) (Chap. 7, Section 8)

(xiv) 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.)?

To our knowledge there are no code of ethics concerning data processing per se.

However, a Research Council's report on Good Research Practices, which covers all ethical issues related to research tackles among other the question of the processing of personal data. In fact, the report mentions the "key legislation and other regulations with which researchers should be familiar", i.e. including the European Data protection legislation and two national regulations, the Patient Data Act and the Act on Ethical Review. The Book mostly explains the gist of the regulations.

Additionally, one may say that the application, that has to be filled by the applicants within the ethical review procedure, indirectly generates awareness of ethical issues related to data processing. [More on the application under Part 5.]

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

The Data Protection Act doesn't define "statistical purposes" but specifies cases in which processing sensitive data for statistical purposes is permitted.

Indeed, according to Chapter 3, Section 7, "Sensitive personal data may be processed on the basis of Article 9 (2) (j) of the EU Data Protection Regulation, if the processing is necessary for statistical purposes and the public interest in the statistical project in which the treatment is included clearly outweighs the risk of undue intrusion into the personal privacy of the individual".

Additionally, the DPA states that personal data that is processed solely for statistical purposes may be used for taking action on the data subject only if there are special reasons for the data subject's vital interests (Chap. 4, Section 2).

(xvi) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The Data Protection Act lays down a limitation of the use of personal data processed for research purpose. Indeed "personal data that is processed solely for research purposes may be used to take action on the data subject only if there are special reasons for the data subject's vital interests" (Chap. 4, Section 3).

The Ethical review Act which applies to research projects, including the processing of sensitive personal data, requires the applicants to carry out a kind of Data Protection Impact Assessment. [For more details see Part 5]..

27.1.2 Rights of data subjects and data processing

(v) 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.

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

None that we are aware of.

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

A characteristic of the Swedish data protection legislation is its relationship to "freedoms of opinion". This is reflected in Chapter 1, Section 7 of the DPA which states "Neither the GDPR nor this Act shall apply so far that they will infringe upon the or the Freedom of expression Act".

This means more precisely that the Freedom of the Press and the Freedom of expression, as well as the Right of access to information, which is regulated by the Freedom of the Press Act, suggest a higher rank than the data protection legislation.

This provision was subject to controversy during the legislative procedure of the Act (2018:218) with supplementing provisions to the EU Data Protection Regulation (DPA). The Swedish Data Protection authority was among the actors raising their voice against such a provision.

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

The general national regulation, the DPA, contains provisions limiting some of the data subjects' rights.

The DPA contains, under Chapter 5, with the heading Limitations to certain rights and obligations, two provisions containing limitations to the right of information and the right of access to information. The first provision states the non-application of these rights to data that the data controller may not disclose to the data subject by law or other statute or by a decision that has been notified under the constitution. The exemption applies even when data controllers are not a public authority, when the data would have been classified as secret by an authority in accordance with the Publicity and Secrecy Act (Offentlighet- och sekretesslagen (2009: 400))

The second provision states that the right of access does not apply to personal data in running text that has not been finalized, when the request was made, or which constitutes a memo or similar. This exemption doesn't apply however to personal data that has been disclosed to third parties; processed solely for archival purposes of general interest or statistical purposes; or has been dealt with for longer than one year in running text that has not been finalized.

When it concerns research, the Swedish legislation does not provide yet for specific cases of exemptions from articles 15, 16 18 and 21 as permitted by Art.89.3 of the GDPR. However, the Research Data Act, drafted but not yet adopted, laid down exceptions from article 16 and article 18.

27.1.3 Minors, sensitive data and other additional categories of data

(iv) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

No.

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

The Data Protection Act (Chap. 4, Section 4), states that when offering the information society services directly to a child living in Sweden, processing of personal data should be permitted with the support of the child's consent, if the child is at least 13 years of age. If the child is under 13, such processing should be allowed only if consent is given or approved by the parent who has parental responsibility for the child.

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

No.

27.1.4 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 general protection for the processing of personal data ceases to apply when a person dies, but in some special legislation it can be stated that the processing of the deceased's personal data must also take place in a certain manner in that legislation, see e.g, the Road Traffic Data Act (Vägtrafikdatalagen (2019:369)), Chap. 1, Section 3, which states provisions on the processing of personal data that also shall apply to deceased persons.

27.1.5 Accountability and Data Protection Impact Assessment

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

As mentioned earlier there is an Ethical Review Authority (Etikprövningsmyndigheten) with the task to carry out an ethical review of processing of personal data for research purposes.

In the security field there is an oversight body concerning the Security Service's processing of personal data.: The Swedish Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden).

(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?

There are no national regulations on this beside the list[222] adopted by the Swedish Data Protection Authority (Datainspektionen) for complying with Art 35.4 GDPR. After an enumeration of criteria, the list contains "examples of processing operations that require an impact assessment to be carried out". Among these examples two, placed under the heading "sensitive data", concern data processing in research:

"Processing including storage for archiving purposes, of pseudonymized sensitive personal data that refers to data subjects from research projects" and "Organisation that collect and store sensitive data in order to serve as basis for future research purposes"..

27.2 Commercialization of data

27.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Lag om avtalsvillkor i konsumentförhållanden (1994:1512) **(Law on contract terms in consumer condition)**	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/marknadsforingslag-2008486_sfs-2008-486 (Swedish)	Hard law	Mainly concerns personal data insofar as commercial personal data processing in consumer contracts may constitute an unfair contractual term.

[222] https://www.datainspektionen.se/globalassets/dokument/beslut/list-regarding-data-protection-impact-assessments.pdf

Marknadsföringslagen (2008:486) **(The Marketing Act)**	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-19941512-om-avtalsvillkor-i_sfs-1994-1512 (Swedish)	Hard law	Mainly concerns personal data insofar as commercial personal data processing in contravention of the GDPR can constitute an unfair business method.

Main regulatory tools addressing data commercialization in Sweden.

27.2.2 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)?

To our knowledge there are no limitations regarding this. However, it is conceivable that such agreements could be infringed on the basis of Section 36 of the Contract law (Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område) if they are considered unreasonable or prohibited by a penalty under the Law on contract terms in consumer condition (lag (1994:1512) om avtalsvillkor i konsumentförhållanden).

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

Yes, it often seems to be the case that users, as part of gaining access to a service, must provide some personal information.

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

There are no specific rules on this, but the Copyright Act (lag (1960:729) om upphovsrätt till litterära och konstnärliga verk)contains rules on non-profit rights if the data constitutes an intellectual and original work.

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

None that we are aware of.

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

No.

27.2.3 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?

Data is not classified into any specific category; it depends on the use that occurs with the data. Data that achieves copyright protection can be protected by the Copyright Act and corporate secrets through the Business Secrets Act.

(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?

If the data constitutes an intellectual and original work, it's protected through the Copyright Act.

When determining the compensation, particular attention should be paid to loss of profit, profits made by the person who has committed the infringement or the violation damage to the reputation of the work non-material damage, and the interest of the author or rights holder in infringing not being made. (Copyright Act, Section 54)

27.3 Security and cybersecurity

27.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
ISO 27000	https://www.sis.se/iso27000/	Soft law (Only recommendations but should be followed by the authorities.)	Provides a structured and effective way of working for organizations that strive for improved internal control over information security
Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster **(Act on information security for essential services and digital services) (NIS)**		Hard Law	Constitutes the transposition act of the NIS Directive

Main regulatory tools addressing security and cybersecurity in Sweden

27.3.2 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 by the Act on information security for essential services and digital services- NIS Act (lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster) that came into force on 1 August 2018. The NIS act is complemented by the Ordinance on information security for essential services and digital services (förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster).

(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 NIS and other regulations such as the Protective Security Act (säkerhetsskyddslagen (2018:585) contain several provisions on technical and organisational measures but those are not connected to the protection of personal data. Most of the prevention falls back on the GDPR.

27.3.3 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?

The obligations for providers of important social services and for digital service providers to report incidents laid down in the NIS Act and its Ordinance state do not refer to personal data breaches. No reference to GDPR is made in the NIS legislation.

Interestingly, during the procedure of transposition of the NIS Directive

some actors put forth the difficulty in the practice that could arise from simultaneous similar requirements from other regulation, such as the GDPR.

1.4.1.2 Supervision of cybersecurity

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

Yes, the NIS Act lays down provisions on supervisory authorities which ensure compliance with the NIS legislation.

(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 supervisory authority in the field of digital infrastructure and digital services, PTS, the Swedish Post and Telecom Authority (Post- och telestyrelsen) which monitors the electronic

communications and postal services, receives notifications from suppliers of essential services. It is endorsed with investigative powers, may issue orders to constrain the providers to fulfil the requirements for security measures and incident reporting. The investigative powers and the injunctions may be combined with a fine. The supervisory authority may also in some cases levy administrative fines. The Authority is also in charge of providing information and guidance concerning the NIS Directive and may issue regulations.

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

Claims relating to damages caused by lack of cybersecurity may be lodged to the first court of instance (tingsrätten), on the basis of the Tort Liability Act (skadeståndslagen (1972:207) or art 82 of GDPR, when personal data are involved.

27.4 Enforcement: fines and sanctions

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

Swedish legislation contains two defined IT crimes;

Data breaches (dataintrång), the Criminal Code (Brottsbalken (1962:700)) Chapter. 4, Section 9 c

Computer fraud (datorbedrägeri), the Criminal Code (Brottsbalken (1962:700)) Chapter 9, Section 1, Section 2.

Data breaches are defined as those who illegally prepare for access to a task that is intended for automated processing or illegally modify, delete, block, or register for such a task. For breaches, the penalty can be fines or imprisonment up to 2 years. In the case of a serious crime, the highest penalty is imprisonment for 6 years.

Computer fraud means that someone leaves inaccurate or incomplete information, by changing the program or recording or otherwise illegally affecting the outcome of an automatic information processing or other similar automatic process. For computer fraud, the sentence can be 2 years in prison and in case of a serious crime 6 years in prison.

Both crimes are primarily aimed at registers and systems for automatic processing.

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

Yes. The Data protection Act states in Chapter 6, Section 2 that administrative fine shall be set at a maximum of SEK 5,000,000 for violations referred to in Article 83 (4) of the GDPR and to a maximum of SEK 10,000,000 for violations referred to in Articles 83 (5) and 83 (6) of the Regulation.

According to chapter 6, Section 3, the supervisory authority may levy an administrative fine for infringements of Article 10 of the GDPR, Article 83 (1), (2) and (3) of the Regulation shall apply in this case. The amount of the fine shall be determined in accordance with Article 83 (5) of the Regulation.

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

For Data breaches, prosecutors may prosecute without the victim having stated the crime to prosecution, while for Computer fraud (which is not serious), the victim must state the crime to prosecution unless prosecution is required from public view.

27.5 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?

Research projects which imply the processing of sensitive data and data on criminal offences must, according to the Ethical Review Act undergo ethical review by the Swedish Ethical Review Authority before the research starts. This Act apply to research involving living or deceased persons or biological material from humans.

The aspects of data protection review that the Swedish Ethical Review Authority focuses on can be deducted from the application that are to be addressed to the Authority.

These applications must contain information on the kinds of sensitive data that are planned to be processed, the methods, including techniques or processing that will be carried out, the description of the characteristics of the data collected and how their reliability is ensured and information about how the collection of data will be carried out, how the data will be handled and stored.

If pseudonymisation occurs a description of the codification process has to be furnished. Additionally, the applicant must indicate how long the data will be stored, if they will be anonymised, and whether they will be destroyed. The applicant must also describe the risks, such as privacy infringements for the persons included in the 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?

The Swedish Research Council (Vetenskapsrådet), the largest Swedish funding agency, which is tasked with raising awareness for, and disseminating information on, ethics in research, provides a Codex containing guidelines, ethic codes and laws concerning ethics for research in general. The Codex does not provide specific information related to data protection. Nevertheless, some documents, such as the above-mentioned report on Good Research Practices by the Research Council (see part 1) touches upon the data protection issue.

(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?

We are not aware of such national regulations or procedures.