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?

In health research/biomedical sciences, the (above noted) the appropriate governance structures for the carrying out of the research must include: ethical approval by a research ethics committee, assignment of relevant data controller and data processors involved, identification of funders and any other to who data may be shared to (incl. anonymised data) and provision of appropriate training must be provided. Other governance requirements on the management and conduct of the research include the performance of an initial assessment of the data protection implications of the health research and, where required under GDPR, a Data Protection Impact Assessment; in addition to implementing and testing security procedures.

Additionally, in terms of personal data breaches, the data processor must notify the data controller (i.e. the individual/legal entity who controls/responsible for collection/storage/use of personal information), who, in turn, must notify the Data Protection Commission with a description of the breach, likely consequences, planned remedial actions, etc. (unless the personal data breach is unlikely to result in a risk for the relevant individual's rights and freedoms).

Large companies and institutions also need to appoint a data protection officer (DPO)

A Privacy Impact Assessment to identify privacy risks is undertaken if personal data is used or being processed in research.

The Data Protection Commission is the overall data protection authority responsible for upholding the personal data protection rights specified by the GDPR.

Defence and security matters are generally covered in the Data Protection Act 1988/2018 - the Minister for Defence may – in relation to personal data kept by him in relation to the Defence Forces, designate an officer of the Permanent Defence Force who holds a commissioned rank therein to be a controller. [The DPA 2018 serves to repeal the Data Protection Acts 1988 to 2003, except for provisions relating to the processing of personal data for the purposes of national security, defence, and international relations of the State. The collective citation is now 'the Data Protection Acts 1988 to 2018'.]

15 Italy

Denise Amram; Giovanni Comandé (Scuola Superiore Sant'Anna)

15.1 Informed consent

15.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope

Legislative Decree 196/2003	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678 https://www.garanteprivacy.it/web/guest/home_en/italian-legislation	Hard law	Italian code on data protection. Issued in 2003 and amended in 2018
DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" *(in G.U.*	https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true https://www.garanteprivacy.it/web/guest/home_en/italian-legislation#1	Hard law	It amends the previous legislation in light of the GDPR

4 settembre 2018 n.205)			
Ethics rules (Regole deontologiche) on data processing issued under article 20, para 4, Legislative Decree 101/2018	https://www.garanteprivacy.it/web/guest/codice A.1 - "Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (G.U. del 4 gennaio 2019, n. 3); **Ethics rules on data processing concerning journalism** A.2 - Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (G.U. del 15 gennaio 2019, n. 12). Ethics rules on data processing for defensive investigations or the establishment, exercise or defence of legal claims. A.3 - Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica (G.U. del 15 gennaio 2019, n. 12); Ethics rules on data processing for archiving purposes in the public interest or historical research purposes A.4 - "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale" (G.U. del 14 gennaio 2019, n. 11); Ethics rules on data processing for statistical	Soft law.	To adapt procedures on specific data processing in light of the GDPR. They have been issued by the data protection authority. They constitute attachments to the hard law. compliance with these ethical rules is an essential condition for the lawfulness and correctness of the processing of personal data pursuant to art. 2-quater, paragraph 4, of the Italian Data Protection Law.

	purposes within the national statistics system A.5 - "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" (G.U. del 14 gennaio 2019, n. 11); Ethics rules on data processing for statistical purposes or scientific research ones		

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

(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?

No, there isn't.

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

Within the application of the EU Directive 2016/680, by the Legislative Decree 51/2018 (https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg), the Data Protection authority and the General Director of the Security Information Department signed a protocol in order to confirm and enhance the commitment to converge their strategies as already stated in 2013 and in 2017 in light of GDPR.

The aim of the agreement is to collaborate and share information and best practice on cybersecurity.

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Autorità Garante per la protezione dei dati	https://www.garanteprivacy.it/web/guest/home_en	yes	162 (December 2018) https://www.garanteprivacy.it/documents/10160/0/Organigramma+al+26+agosto+2019.pdf/a0b7b223-0c36-0d26-	high	18.557 (period: 25.5.2018-31.5.2019)

			7c6e-378687a435e7?version=1.2		

Information regarding Data Protection Authority in Italy

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

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

"Data processing for research purposes" are the one which are performed by research centres, universities or private companies which include "research" in their statutory.

Research in public interest is not completely defined, however article 110 of the Data Protection Act establishes that consent is not required in case of research established by the law and whereas it is performed by Hospitals and Clinics who joined a specific biomedical or medical program launched under article 12bis of the Legislative Decree 502/1992 n Act in 1997. In this case a DPIA should be performed and published.

The distinction between public or private bodies is not relevant if the private body pursues research purposes as core-activity and it emerges from its statutory.

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

No, but within the CODAU (the Conference of the General Directors of Public Administration within the Universities), a group of DPO started an intensive dialogue in order to harmonize standards and share best practices.

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

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

Articles 104 ff. of the Data Protection Act as amended by L.D. 101/2018 refers to data processing for statistical and scientific research purposes. These articles specify principles that shall orient the data protection authority while drafting the Ethics code on the topic. For statistical purposes, article 2 of the Ethics rules on data processing for statistical purposes under the national statistics system issued by the data protection authority refer to "processing for statistical purposes" as "any processing carried out for the purposes of statistical investigation or production, storage and dissemination of statistical results under the national statistical program or to carry out statistical information in accordance with the institutional areas of the bodies referred to in Article 1." In this context, data are aggregate if the data subject is not re-associated under at least

3 units, considering the level of confidentiality of the information. In case of sensitive data under article 9 and 10 GDPR, the national statistical plan shall illustrate purposes and measures to be applied, prior the data protection authority opinion.

Specific ethics rules have been issued for data processing for statistical purposes performed by the National Statistics Institute (ISTAT).

In particular, answers can be provided from third parties respect to the data subject whereas the latter cannot participate to the survey. Consent can be collected by simplified means. Data are considered aggregate if they respect specific levels (i.e. under 3 units, considering the specific context and the intensity). Researchers must respect specific confidentiality commitments.

15.1.2 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.)

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

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

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

Article 2 quinquies of the Data Protection Act states that the consent under article 8 GDPR can be expressed by 14yrs old minors. Parents (or the ones who exercise parental responsibilities may give consent on behalf of children under 14yrs old). In that case, information should be particularly user-friendly.

As far as data subjects' rights are concerned, Article 2 undecies of the Data Protection Act illustrates whereas they can be limited. In particular, this could happen in case of interests protected under AML legislation, or to protect extortion victims, in case of parliamentary committees of inquiry; in case of activities carried out by a public entity, which are not economic public bodies, but that are based on the express provision of law, for exclusive purposes related to monetary and currency policy, to the payment system, to the control of intermediaries and credit and financial markets, as well as to protect their stability; or to protect the whistle-blower under the Legislative Decree 179/2017.

15.1.3 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)?

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

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

Not directly. However, as far as health data are concerned, the Italian data protection authority clarifies the legal bases for health data processing, establishing for example that consent is necessary in case of access to healthcare apps, to the health care records, or in case of online medical report transmission, or in case of fidelity cards involving patients,

as well as other activities relating to marketing or commercial purposes, or electoral ones (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942).

Another vulnerable category refers to workers. In particular, as far as surveillance is concerned, article 4 of the Workers Act n. 300/1970 specifies that video surveillance system in workplace should be agreed by trade-unions or by the competent authority (Ispettorato del Lavoro).

15.1.4 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?

Article 2 terdecies of the Data Protection Act states that data subjects' rights can be exercised by those who have a personal interest, or behave to protect the deceased data subject, on his behalf, or for family reasons that shall be protected. This is true unless the data subject has expressly prohibited it. In any case, the data subject can withdraw his/her prohibition anytime. Prohibition cannot affect economic interests of third parties as well as the right to defence.

This provision has to be balanced with other rights. In the past, the Data Protection Authority has prohibited the daughter of a poet to access his email account in order to protect the opposite fundamental right relating to the mail confidentiality of third parties. The same balance brings to distinguish between job email accounts (like the non-personal one) and possible dual-use of the same account.

15.1.5 Accountability and Data Protection Impact Assessment

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

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

The ethics rules issued in the given areas identify procedures to fairly process data for specific purposes. These procedures refer to organizational measures that data controller has to implement in order to be accountable. As above-mentioned specific ethics rules refer to scientific research and statistics.

15.2 Commercialization of data

15.2.1 General Regulatory Framework

There is not a specific regulatory framework for data commercialisation in Italy

15.2.2 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, it does follow the principles stated by the GDPR.

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

We suppose yes.

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

No, it doesn't.

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

Article 110bis of the Italian Code refers to secondary use for research and statistical purposes, regulating the procedures to follow in case that data subjects could not have been informed because of specific reasons or that was impossible. In this case, a prior consultation to the data protection authority should be performed as well as there is a general provision on the topic. Furthermore, article 110 bis states that the described procedure cannot be applied to secondary use for research purposes of health data collected for healthcare purposes by hospitals and clinics.

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

No, we don't.

15.2.3 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?

Personal data are a controversial category: it shall be protected, but it has also an economical value which contributes to the market once processed. The balance between fundamental rights allows to identify how to protect data without limiting their circulation. In general, in B2C market data are processed under the performance of a service.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Yes, the Copyright Act 22.4.1941 n. 633.

15.3 Security and cybersecurity

15.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
D.Lgs. 18 maggio 2018, n. 65 Attuazione della	https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg	Hard law	It implements principles

direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092) (GU Serie Generale n.132 del 09-06-2018)			stated in the NIS directive
Codice Amministrazione digitale D.Lgs. 7.5.2005 n. 82	https://www.camera.it/parlam/leggi/deleghe/testi/05082dl.htm	Hard Law	It includes rules on digital transition of public administration
Circolare AgID n.2/2017 sulle "Misure minime di sicurezza ICT per le pubbliche amministrazioni"	https://www.gazzettaufficiale.it/do/atto/serie_generale/caricaPdf?cdimg=17A0306000100010110003&dgu=2017-05-05&art.dataPubblicazioneGazzetta=2017-05-05&art.codiceRedazionale=17A03060&art.num=1&art.tiposerie=SG	Hard Law, secondary law.	It includes technical measures for public administration
"Linee guida sulla formazione, gestione e conservazione dei documenti informatici" AGID		Soft Law, but binding for public administration	They update article 71 Codice Amministrazione Digitale on the management and storage of data included in digital format

Main regulatory tools addressing security and cybersecurity in Italy

15.3.2 Implementation of EU Law

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

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

(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?

NIS directive has been in implemented under Legislative decree 65/2018. It is applicable to essential service operators and digital services suppliers.

15.3.3 Personal Data Breach Notification

(ii) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

Yes, it is. Each event which can concretely affect the capacity of a network and the resilience of an informative system, considering a given level of confidentiality, each actions which compromise the availability, integrity and confidentiality of data processed and related offered services should be communicated to the Computer Security Incident Response Team.

15.3.4 Supervision of cybersecurity

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

(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?

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

The Computer Security Incident Response Team has advisory, information, and coordination powers. Its members are appointed under the suggestion of the involved Ministry.

In Particular, the CSIRT:

- it illustrates procedures on data breach preventing and management;

- it receives the data breach reports and informs the DIS (Security Information Department) in order to prepare and prevent possible critical situations and to activate emergency procedures that should be implemented by the Nucleo per la sicurezza cybernetica;

- it informs the other Member States possible involved in the breach, in order to protect safety and commercial interests of the Essential Services Operators an Digital Services Suppliers as well as confidentiality of the provided information

- it ensures the cooperation within the CSIRT network though best practice and guidelines.

Competent authorities may condemn to pay a fine up to 150.000 euros

15.4 Enforcement: fines and sanctions

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

Both. it depends from the offence (such as the false statement to the data protection authority, fraudulent acquisition of large-scale personal data)

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

Yes, there are.

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

It depends on the offence: the ones that are originated by a control from the data protection authority are official one (e.g. article 167 ff. of the Data Protection Act), the ones included in the criminal code are prosecute by the injured parties.

15.5 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?

(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?

(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?

A critical issue arises from the article 110 of the Italian Data Protection Act that introduces data processing for research purposes medical, biomedical, and epidemiological purposes. In fact, it states that the consent of the data subject is not necessary whereas article 9, para 2, sub j) is applicable, or if it is impossible to inform because of exceptional causes, or to

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

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

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

16 Latvia

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

16.1 Informed consent

16.1.1 General Regulatory Framework

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