The author has found no indication that German research funding agencies (or other research supporting bodies) facilitate data protection by means of particular tools, or guidelines for the implementation-phase of research projects. That said, German funding institutions at federal and state level increasingly incorporate ethical, legal, and social aspects (ELSA) into their funding programs. This can either constitute projects of their own focussing on data protection research, parts of projects (e.g., as a work package), or calls for coordination and support activities that run alongside a set of research initiatives with a common topic (e.g. the project "Assessing Big Data" ABIDA[118] as an interdisciplinary research project on legal, ethical and economical aspects of big data). A long-lived and cross-sectional and interdisciplinary project which addresses data protection from various angles is the project "Privacy Forum and Self-determined Life in the Digital World"[119] which is funded by the Federal Ministry for Education and Research.

(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 author is not aware of specific national procedures and regulations applicable to ICT R&I but the University and College legislation of several federal states and the public research institutions themselves have limitations on research with dual use potential. In Germany, the EU Dual Use Regulation (EC) 428/2009 is applicable, however. The body responsible for its enforcement is Federal Office for Economic Affairs and Export Control ("Bundesamt für Wirtschaft und Ausfuhrkontrolle", BAFA). The BAFA published guidelines titled "Export Control in Science & Research" as well as the "Export Control and Academia Manual".[120]

Regarding the protection against industrial espionage, the author is unaware of any particular tools. Guidance and support for researchers in academia and industry is available from the Offices for the Protection of the Constitution ("Verfassungsschutzamt") at both, federal and state level. All institutions and offices in charge of counter intelligence also offer advice, guidelines, and instructions to researchers and businesses.

12 Greece

Irene Kamara (Tilburg University)

12.1 Informed consent

12.1.1 General Regulatory Framework

[118] See https://www.abida.de/en.
[119] See https://www.forum-privatheit.de/en/.
[120] Download page for both publications, https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Academia/academia_node.html.

Regulation	Link	Type of regulation	Brief description and scope
Law 4624/2019 Data Protection Authority, adaptation measures for the protection of natural persons against the processing of personal data in Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016, and implementation of the Directive 680/2016 of the European Parliament and the Council of 27th April 2016, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προσαρμογή της εθνικής νομοθεσίας για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016.	http://www.et.gr/idocs-nph/pdfimageSummaryviewer.html?args=sppFfdN7IQP5_cc--m0e1waP6hGUu9dixw0NNhu3Ppm8rzSZFxgk-XLICQIaWE9-kAYi3ORfmarM6Ym_fEOTFvdTgs9wBKVx4kicnjz_3u4G8qOBlZzQoc77k1-A9Eyz7vqZ2xJ5_DbhyWTxXzY2LOXriDDKalMPz4Pwwo55CqRzraQl-zQzGw..	Formal law	Comprises of 87 Articles, refers to both GDPR and Law Enforcement Directive (LED) 680/2018. The scope of application is the same as the one defined in Art. 1 GDPR and Art. 1 LED.
Law 3471/2006, Protection of personal data and privacy in the electronic communications sector and amendment of law 2472/1997, GG A, 113/28.06.2006, amended by Law 4070/2012, Regulations on electronic communications, transport and public works, GG A' 28/10.04.2012	https://bit.ly/2MR2JMi	Formal law	The implementation law of the Directive 2002/58/EC, as amended by Directive 2009/136/EC.

ΝΟΜΟΣ 3471/2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997, ΦΕΚ 133/Α'/28.6.2006.			
Civil Law Code (Αστικός Κώδικας)	N/A	Codified law	General concept of consent in civil law

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

(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?

We are not aware of such provision, apart from the constitutional protection of the processing of personal data which applies to processing independently of purely personal or household activity.

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

We are not aware of such legislation dedicated to data protection and national security. However, fragmented provisions are introduced in several security related laws. Content wise, they do not add much. They mainly refer to the observance of the national data protection law, where applicable.

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Hellenic Data Protection Authority	https://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL	yes. Its independence is established in the Constitution (Article 9A)	Around 60 persons	As active, as its budget limitations allow.[121]	See latest Annual Report 2017, p.28f: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/

[121] See July 2019 Newsletter with activity: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/INFORMATIONAL/JULY2019.PDF

					ANNUAL%202017_WEBPAGE.PDF

Information regarding Data Protection Authority, Greece

(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.?

The aforementioned laws under Table 1 do not introduce a specific definition.

(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 aforementioned laws under Table 1 do not introduce such a definition.

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

Art. 22 of Law 4624/2019 regulates the processing of special categories of personal data. Art. 22(1) introduces three deviations from Art. 9 (1) GDPR, when such data are processed by either private or public sector organisations:

a. the exercise of social security rights and the fulfilment of relevant obligations (Art. 22(1)(a)),

b. preventive medicine purposes, the evaluation of working capability of an employee, medical diagnostics, the provision of health or social care or the operation of social care or healthcare systems and services or on the basis of a contract with a healthcare professional or a person bound by professional secrecy or a person under the supervision thereof (Art. 22(1)(b)),

c. purposes of public interest in the public health sector, such as serious cross-border threats against health or for safeguarding high quality and safety standards in healthcare, medication, or medical devices. In addition to the measures provided in Art. 22(3), for the cases under 22(1)(c) the provisions on professional secrecy imposed by law or code of conduct should be observed. (Art. 22(1)(c)).

Art. 22(2) introduces further deviations from Art. 9(1) GDPR for processing of personal data belonging to special categories, when processing is performed by the public sector. The four cases are: a. when the processing is absolutely necessary for substantial public interest purposes (Art. 22(2)(a)), b. when the processing is necessary for the prevention of a significant threat against national or public security (Art. 22(2)(b)), c. when the processing is necessary for taking humanitarian aid measures (Art. 22(2)(c)). An additional requirement for all the four cases is that the interest of the data controller outweighs the data subject interest.

In all the above deviations, introduced in Art. 22(1) and (2), appropriate and special measures for the protection of the data subject interests need to be taken. Art. 22(3) provides a non-exhaustive list of such measures, which need to take considering the state of art in technology, implementation costs, and the nature, extent, context and purposes

of processing, as well as the risks, depending on the severity the processing imposes on the rights and freedoms of natural persons. The measures of Art. 22(3) are:

a. technical and organisational measures that ensure that the processing is performed in line with the GDPR. b. measures that enable the verification and determination a posteriori whether and by whom the personal data have been introduced, modified, or removed. C. measures to strengthen awareness of the personnel involved in the processing. d. access limitations to data controllers and processors e. the use of pseudonyms for the personal data. f. cryptography g. measures for safeguarding the capacity, confidentiality, integrity, availability, resilience of the systems and services relating to the processing of personal data, taking into account the capability of fast restoration of the availability and access in case of a physical or technical incident. h. processes for the regular testing, assessment, and evaluation of the effectiveness of the technical and organizational measures for safeguarding.

(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.)?

Law 4521/2018 obliges academic institutions to establish Committees of Ethics of Research.[122] Those Committees usually abide by different Codes of Ethics, developed in each academic institution. Such Codes of Ethics commonly follow a similar structure: General principles and scope, synthesis and operation of the Committee of Ethics of Research, Special rules on research/testing in relation to humans, animals, natural/habitat/cultural environment. Some Codes refer to the protection of personal data and protective measures such as codification, secure storage of data, access management, de-identification during the processing of the data or the publication of results.[123]

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

No. It should be highlighted however that the legislative proposal refers to purposes of collection and retention of statistical data ('για σκοπούς συλλογής και τήρησης στατιστικών στοιχείων') (Art. 30) instead of 'statistical purposes' which is the wording in Art. 89 GDPR and its translation in Greek ('στατιστικούς σκοπούς').

(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.)

See reply to previous questions on Art. 30 of the national law.

12.1.2 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.)

There are several sectoral national laws referring to data processing. Nonetheless in relation to the GDPR transposing law we are not aware of particularities regarding data subjects.

[122] N. 4521/2018 (ΦΕΚ A 38/2-3-2018) Ίδρυση Πανεπιστημίου Δυτικής Αττικής και άλλες διατάξεις.

[123] See for example art. 14 of the DUTH Code of Ethics: http://ethics.duth.gr/duth_code.html

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

Nothing that deviates from the GDPR.

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

Art. 30(2) of the national law adapting national legislation to the GDPR (Law 4624/2019) introduces limitations to the exercise of the data subject rights, when their exercise in the case of processing for scientific or historical research or statistical purposes might seriously impede those purposes. For the same reasons, Art. 15 GDPR right of access by the data subject does not apply when the personal data are necessary for scientific purposes and the provision of information to the data subject would require disproportionate effort.

Conditioned limitations to the application and exercise of the right of access are introduced in several provisions: Art. 30(2), Art. 29(2) for processing for archiving purposes in the public interest, and Art. 33. The latter which refers to cases such as 1. that the personal data is recorded only for the reason that it is not possible to be erased due to legal or other regulatory provisions that demand their retention (Art. 33(1)(b)(aa)) or the data are serving solely purposes of protection or control of the data (Art. 33(1)(b)(bb)). In the cases of limitations introduced in Art. 33(1), there is an additional condition imposed by the legislator, that is that the provision of information to the data subject would entail a disproportionate effort for the data controller and the technical and organizational measures render it impossible to process the data for other purposes.

Art. 34(1) introduces conditioned limitations to the application and exercise of the right to erasure in the case of non-automated processing, when the nature of storage is such that does not allow erasure or requires disproportionate significant effort. In such case, the right to erasure does not apply, and the data subject may use the right to restrict processing in line with Art. 18 GDPR. The Art. 34(1) limitation does not apply in case of illegal processing.

The right to object does not apply in the case of a public sector organisation, when there is an urgent public interest in processing the personal data. The public interest needs to outweigh the interests of the data subject or the processing is mandated by law. (Art. 35 of the national law).

12.1.3 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)?

No. There was a provision in the legislative proposal of August 2019, but it was not included in the final text of the Law. According to Art. 21(3) of the legislative proposal, the data controller would need to put reasonable efforts, taking into account available technological means, to verify that consent of a minor is provided by its legal guardian on his/her behalf.

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

According to Art. 21(1) of the legislative proposal for the Protection of Personal Data applying the Regulation (EU) 2016/679 the minor can provide consent after the 15th year

of age. Under the 15th year of age, the processing is lawful only with the consent of the legal guardian.

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

There is no reference to vulnerable individuals in the legislative proposal for the Protection of Personal Data adapting the national legislation to the Regulation (EU) 2016/679.

12.1.4 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?

We are not aware of specific rules on this matter.

12.1.5 Accountability and Data Protection Impact Assessment

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

The only reference to accountability of Art. 5 GDPR is found in Art. 8 of the relevant national law which refers to the obligation of the data protection officer to monitor the compliance with the provisions of the current law and any other laws with data protection provisions, as well as policies of the public sector.

(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 examined legislation does not prescribe particular requirements for data protection impact assessments in relation to the GDPR (it does so in Art. 65 Law 4624/2019 only in relation to the Directive 680/2016).

12.2 Commercialization of data

12.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Civil Code (Αστικός Κώδικας)	N/A	Codified law	Art. 57 – Right to personality
Criminal Code (Ποινικός Κώδικας) **Νόμος 4619/2019 – ΦΕΚ 95/A/11-6-2019, όπως τροποποιήθηκε με**	N/A	Codified law	Chapter 22 – Violations against privacy and secrecy of communications [Articles 370, 370A, 370B, 370D, 370E, 371].

Πράξη Νομικού Περιεχομένου της 27-06-2019 – ΦΕΚ 106/A/27-06-2019 και διορθώσεις σφαλμάτων όπως δημοσιεύθηκαν στο ΦΕΚ 122/A/16-07-2019.			

Main regulatory tools addressing data commercialization in Greece.

12.2.2 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)?

This seems to be the common practice throughout the EU, but the contracts (Terms&Conditions) are not formally drafted in a manner that this is.

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

See above.

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

We are not aware of such regulation.

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

We are not aware of such regulation, except for what is regulated with the data protection legislation.

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

Since metadata are personal data, they are protected via the data protection legislation. The Regulation on the free flow of non-personal data applies (Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union).

12.2.3 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 would rather be considered as an aspect of personhood and personality rights.

(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?

We are not aware of any formal mechanisms to determine the value of data.

12.3 Security and cybersecurity

12.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law 4577/2018 Incorporation into Greek legislation of Directive 2016/1148 / EU of the European Parliament and of the Council on measures for a high common level of security of network and information systems across the Union and other provisions, GG A 199/03-12-2018 **Νόμος 4577/2018 Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις, ΦΕΚ Α' 199/03-12-2018.**	https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html	Hard law	Implementation of the Network and Information Security Directive 2016/1148 / EU.
National Cybersecurity Strategy (rev.3)	https://diavgeia.gov.gr/doc/%CE%A84%CE%A17465%CE%A7%CE%980-%CE%966%CE%A9?inline=true	Hard law	National strategy on the security of network and information systems
Law 4624/2019 Data Protection Authority, adaptation measures for the protection of natural persons against the processing of personal data in Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016, and implementation of the Directive 680/2016 of the European Parliament and the Council of 27th April 2016, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προσαρμογή της εθνικής	http://www.et.gr/idocs-nph/pdfimageSummaryviewer.html?args=sppFfdN7IQP5_cc--m0e1waP6hGUu9dixw0NNhu3Ppm8rzSZFxgk-XLICQIaWE9-kAYi3ORfmarM6Ym_fEOTFvdTgs9wBKVx4icnjz_3u4G8qOBlZzQoc77k1-	Hard law	Comprises of 87 Articles, refers to both GDPR and Law Enforcement Directive (LED) 680/2018. The scope of application is the same as the one defined in Art. 1 GDPR and Art. 1 LED.

νομοθεσίας για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016.	A9Eyz7vqZ2xJ5_DbhyWTxXzY2LOXriDDKalMPz4Pwwo55CqRzraQl-zQzGw..		

Main regulatory tools addressing security and cybersecurity in Greece.

12.3.2 Implementation of EU Law

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

The law 4577/2018 has been published in the Official Gazette in November 2018 and has started applying since December 2018.

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

See previous replies in section one of the questionnaire regarding personal data protection.

In relation to information security, the national implementation law of the NIS Directive (Law 4577/2018) refers to the GDPR when the processed data are personal. (Art. 2 Law 4577/2018).

Art. 11(1) of the Law 4577/2018 provides that the National Cybersecurity Authority in collaboration with the competent CSIRT and other involved parties is evaluating the technical and organisational measures for risk management. Despite the fact that the provision does not refer to specific measures, it provides a non-exhaustive list of elements that are assessed: a. the security of systems and premises b. incident management c. business continuity management d. monitoring, controls, and testing of the networks and information systems e. conformity to international standards.

12.3.3 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?

Art. 11(3) of the national implementation law of the NIS Directive provides that the National Cybersecurity Authority determines the process of data breach notification that the digital service providers need to pursue. In order to determine whether the impact of the breach is severe the duration of the incident, the geographical scope of the affected

area, the degree of disturbance of the functioning of the service, and the extent of the consequences on the financial and social activities, need to be taken into consideration

12.3.4 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?

The Law 4577/2018 (NIS transposition) establishes the National Cybersecurity Authority (Art. 10). The Authority assesses the compliance of the regulatees, and may issue binding guidance to the regulatees that have been found to have inadequacies. The Authority belongs to the administration of the Ministry of Digital Policy, Telecommunications, and Information (http://mindigital.gr/).

In addition, there is the Directorate of Persecution of Cybercrime (Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος) (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194EN EN) which is a directorate of the Greek Police, reporting directly to the Chief of Greek Police. Its mission includes the prevention, investigation and suppression of crimes or antisocial behavior, committed through the Internet or via other electronic means of communication. The Directorate consists of several departments related to its core competences: innovation and strategy department, department for the security of electronic and telephone communication and protection of software and intellectual property rights, department of protection of minors on the Internet and digital investigation, department of special cases and Internet white collar crime, administrative support department.

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

The means to claim damages largely depends on the type of offense committed.

12.4 Enforcement: fines and sanctions

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

Crimes related to data protection: As provided in Art. 38 of the national law adapting national legislation to the GDPR, punishes criminal offences with imprisonment up to 1 year. Depending on certain conditions prescribed in Art.38, the offences are considered felonies and punished with more stringent penalties. An example is when the offence concerns personal data that belong to the special categories of Art. 9 GDPR or Art. 10 GDPR. The crime then is considered a felony and is punished with imprisonment up to 10 years and pecuniary penalty up to 100.00 euro (Art. 38(3)). Another example of such conditions is found in Art. 38((5) Law 4624/2019, according to which, in case the actions

of the previous paragraphs pose a risk to the free functioning of democracy or the national security, there is a penalty of 25 years imprisonment and pecuniary penalty up to 300.000 euro.

Crimes related to confidentiality of communications: As provided in Art. 370A, 370B, 370C of the Greek Criminal Code are punished by both imprisonment and pecuniary penalties.

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

There is an interesting decision of the HDPA (nr.26/2019) according to which a fine of 150.000euro was imposed to a multi-national auditing company, together with the obligation to take corrective actions in order to comply with Art.5 (1)(a) and (2), and Art 6(1) GDPR.

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

It depends on the type of crime. When a data protection offence constitutes a felony, it is prosecuted *ex officio*.

12.5 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?

As mentioned in a previous question, every University and public research forum in Greece is obliged by law to establish Committees of Ethics of Research ("Επιτροπή Ηθικής και Δεοντολογίας της Έρευνας"). Such Committees are reviewing among other things whether a research project respects privacy and the protection of personal data of the participants (Art. 21(2) Law 4521/2018, as updated with the Law 4611/2019). The project proposals are either approved by the Committee or the competent Committee issues recommendations and proposes its revision, in case there are ethical or deontological

issues. The decisions of the Committees are binding. Especially for the cases of research projects involving research on humans, or genetic material, cells and personal data, on animals or natural and cultural environment are mandatorily submitted to the Ethics Committees for review and they are not allowed to start before an approval from the Committee. Apart from such cases, the Committees may examine a research project upon request or complaint.

The practices regarding the provision of instruments differ depending on the organisation/University. For example, the University of Patras provides a list of questionnaires (forms) and regulations for the researchers as guidance. Those include questions on personal data protection such as the technical and organisational measures for the protection of personal data. Researchers are also required to submit to the committee the template for the consent form. Guidance on the necessary elements of the consent form is already provided in another document ('Regulations').

Other than those Committees imposed by Law 4521/2018, there is the National Bioethics Commission (Εθνική Επιτροπή Βιοηθικής). The National Bioethics Commission has an advisory role to public sector institutions. It provides its reports and opinions on its own initiative or upon request.

In Greece, there is a centre for Research and Technology for National Defence ('Κέντρο Έρευνας και Τεχνολογίας Εθνικής Άμυνας'), which is established by law (Law 2919/2001). It is subject to the Ministry of Defence. Further, there is the Council of Research on Defence, Technology, and Industry ('Συμβούλιο Αμυντικής Έρευνας, Τεχνολογίας και Βιομηχανίας') which is an advisory board to the Ministry of Defence (established by Law 2919/2001, as amended by Article 33 Law 4609/2019) on matters of research and technology policy of the country, collaboration with academic institutions, major research projects on defence and technology. However, to our knowledge, there is no publicly available information on the tools the researchers are using on security-sensitive technologies.

13 Hungary

Jóri András Ügyvéd (Dataprotection.eu Ltd.)

13.1 Informed consent

13.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
The Fundamental Law of Hungary (Constitution)	http://njt.hu/translated/doc/TheFundamentalLawofHungary_20190101_FIN.pdf	act (hard law)	Article VI of the Constitution governs the fundamental rules of the protection of privacy and personal data and sets out that the activity of an independent supervisory authority to be regulated in a cardinal act.