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.

Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Privacy Act)	http://njt.hu/translated/doc/J2011T0112P_20190426_FIN.pdf	act (hard law)	The Privacy Act is the general background legislation. The purpose of this Act is to lay down, in the areas falling within its scope, the fundamental rules for data processing in order to ensure that natural persons' right to privacy is respected by controllers, and to achieve the transparency of public affairs through the enforcement of the right to access and disseminate data of public interest and data accessible on public interest grounds. The Privacy act regulates the areas beyond the scope of the GDPR, in general the provisions of the Act follow the ones of the GDPR. The territorial scope of the Act is regulated in line with the GDPR as follows: unless otherwise provided by an Act or a binding legal act of the European Union, the provisions of this Act laid down in paragraph (2), as well as other provisions prescribed in an Act on the protection of personal data and on the conditions of processing personal data,, shall apply to the processing of personal data under the GDPR if a) the controller's main establishment specified in Article 4 point 16 of the GDPR or its single establishment within the European Union is in Hungary, or b) the controller's main establishment specified in Article 4 point 16 of the GDPR or its single establishment within the European Union is not in Hungary, but the processing operation performed by the controller or by the processor acting on behalf of, or instructed by, the controller is related to ba) offering goods or services to data subjects in Hungary, irrespective of whether it requires payment by the data subject; or bb) monitoring the data subject's behaviour in the territory of Hungary. Informed consent: the Act provides for the concept and the applicable

			rules of consent and providing information.
Several sector specific acts			Sector specific acts regulate data processing issues in line with GDPR. There may be rules that regulate consent typically beyond the original purposes of data processing.

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

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

Yes, by repeating the same objective in paragraph 6 of Section 2 of the Act: "The provisions set out in this Act shall not be applied to natural persons processing data exclusively for their own personal purposes."

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

The Privacy Act implements Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA as well. Act CXXV of 1995 on the National Security Services and other related decrees regulate data processing of the services. Powers of the Counter Terrorism Centre are regulated by Act XXXIV of 1994 on the Police, however concerning its surveillance activity not relating to criminal investigations, the Police Act refers to the Act on the National Security Services, therefore non-criminal investigatory surveillance by the Counter Terrorism Centre is also regulated by the same Act.

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
National Authority for Data Protection and Freedom of	https://www.naih.hu/general-information.html	Yes	116	Authority annually organizes conference for DPOs as per the requirement	Authority gives responses to enquiries, but emphasize the non-

Information				of the Privacy Act; Staff members participate in conferences for renumeration, which poses integrity issues	binding nature of such positions

Information regarding Data Protection Authority, Hungary

(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.?

Such definition is non-existent; however, an act governs such data processing activities (Act No. CXIX of 1995). According to this act, scientific research is "the activity with the aim of acquiring additional knowledge about the world, where the exploration of the respective societal, economic or natural phenomena needs contact with natural persons or the processing of name or address data".

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

Act No. CXIX of 1995, passed well before GDPR, contains such safeguards. However, the provisions guiding research of the act were not revised in light of GDPR (as opposed to those regulating direct marketing activities).

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

Paragraph 8 of Section 5 of the Privacy Act regulates that an organ or person engaged in scientific research may disclose personal data provided that it is necessary for the presentation of the results of scientific research on historical events.

Act CXIX of 1995 on the use of name and address information serving the purposes of research and direct marketing regulates the concept and requirements of research activities. The act regulates the general rules regarding data processing in relation to scientific research, the exercising of data subjects' rights, and safety of disclosing data. The Act gives detailed rules regarding the content of the research plan, and the plan of data use. According to paragraph 1 of Section 7, scientific researchers, prior to commencing the research projects under the scope of the Act, must prepare a plan of data use. Such plan is to be modified if the purpose of the data use is changed during the research process. The plan of data use must include: a) the entitlement to conduct research, b) the objective of the research, c) the source and sphere of personal data to be used, d) the process of data use, e) guarantees for practical enforcement of the subject party's rights, and f) the technical and organisational measures taken for data protection. The plan must be kept on file in order to provide proof of the legitimacy of the data use

and for inspection until the use of the data is terminated. In the case of institutional scientific research projects, the rights and obligations of the scientific researcher shall fall on and are to be observed by the organisation carrying out the research activity.

Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives regulates the activity of archives and includes provisions on data processing for the purposes of scientific research.

Act XLVII of 1997 on the Processing and Protection of Medical and Other Related Personal Data regulates data processing issues for the purposes of scientific research. Safeguards for the processing of personal data for scientific purposes are the regulations that govern the process of authorisation of the research plan, keeping an access log regarding the data bases and the supervision or oversight of the institution leader and the data protection officer.

(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 specific codes of conduct for data processing for scientific purposes are applicable. Data protection issues regarding scientific research form only a part of a code of conduct covering wider issues. For example, in the Codex of Bioethics on the concepts and practice of biomedical research, there are two paragraphs governing the objective of complying with data protection requirements throughout the research, or the Science ethical code of the Hungarian Academy of Sciences is another good example. Decree 23/2002. (V. 9.) of the Ministry of Health on biomedical research involving human subjects lays down special rules on the protection of persons taking part in the research, providing information about and giving consent to the research, the institutional research ethical committee and the Regional Research Ethical Committee, reporting obligation, provisions on examinations involving no intervention.

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

No. Act CLV of 2016 on Official Statistics is the main legal instrument guiding processing data for statistical purposes. Within this frame personal data may only be processed by the Statistical Office if it is provided for by an act within the given scope of special categories of data

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

As referred to above, Act CXIX of 1995 on the use of name and address information serving the purposes of research and direct marketing includes some rules on performing researches, as presented above, and in sector specific legislation, for example in relation to medical data.

13.1.2 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)?

Sector specific legislation may contain explanatory regulations in this regard, but codification followed GDPR in general. Note, however, the remarks regarding the enforcement of the rights regarding the data of deceased persons below.

13.1.3 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)?

Yes, regarding criminal personal data and processing for law enforcement purposes, including processing of biometric data within this scope, for example.

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

No. According to paragraph 1 of Section 2:12 of the Civil Code: the legal statements of a minor with limited capacity shall not be deemed valid without the consent of that minor's legal representative. If and when a minor of limited capacity becomes competent, he shall be entitled to make his own decisions concerning the validity of his pending legal statement. Pursuant to paragraph 3 of Section 6 of the Privacy Act the statement of consent of minors over the age of sixteen shall be considered valid without the permission or subsequent approval of their legal representative.

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

No.

13.1.4 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?

According to Section 25 of the Privacy Act (1) Within five years of the death of the data subject, the rights to which the data subject was entitled in his life, specified in section 14 b) to e), or in the case of processing operations under the GDPR, the rights specified in Article 15 to 18 and in Article 21 of the GDPR, may be enforced by a person authorised to do so by the data subject in the form of an administrative disposal or a declaration made at the controller and incorporated in a public deed or a private deed of full probative value, taking into account the declaration of the later date if the data subject has made more than one declaration to the same controller. (2) If the data subject has not made a juridical act complying with paragraph (1), his close relative according to the Civil Code may enforce, even in the absence of it, within five years of the death of the data subject, the rights to which the data subject was entitled in his life, specified in section 14 c), or

in the case of processing operations under the GDPR, the rights specified in Article 16 and Article 21 of the GDPR, as well as in section 14 d) and e), or in the case of processing operations under the GDPR, the rights specified in Article 16 and Article 18 of the General Data Protection Regulation, if the processing had already been unlawful in the life of the data subject or if the purpose of processing terminated upon the death of the data subject. The close relative who is the first to exercise his right shall be entitled to enforce the data subject's rights under this paragraph. (3) In the course of enforcing such rights, in particular during the procedures against the controller and before the Authority or a court, the person enforcing the data subject's rights under paragraph (1) or paragraph (2) shall be entitled to the rights and be bound by the obligations laid down in this Act with regard to the data subject. (4) The person enforcing the data subject's rights under paragraph (1) or paragraph (2) shall verify the fact and the date of the data subject's death with a death certificate or with a court decision, as well as his own personal identification, together with his status as a close relative in the case under paragraph (2), with a public deed. (5) Upon request, the controller shall inform the data subject's close relative according to the Civil Code on the measures taken on the basis of paragraph (1) or paragraph (2), unless the data subject had prohibited it in his declaration specified in paragraph (1).

According to the Hungarian data protection legislation the data concerning the deceased data subjects is not treated as personal data, but since conclusions may be drawn on descendants, one has to be cautious when dealing with such data. The provisions of the Code on the right in memoriam are applicable: (1) In the case of any violation of the memory of a deceased person, the relative and/or the person having been named heir apparent in the will of the deceased shall be entitled to bring court action. (2) Any heir shall have the right to lay claim to any financial advantage obtained by having violated the memory of a deceased person. Where there are several heirs, the deprived financial advantage shall be distributed among the heirs according to their respective shares of the estate. Furthermore, Section 228 of the Criminal Code regulates desecration: any person who violates the memory of deceased persons by the means defined in Section 226 (defamation) or Section 227 (slander) is guilty of a misdemeanour punishable as defined therein.

13.1.5 Accountability and Data Protection Impact Assessment

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

Provisions of the GDPR are applicable. The Privacy Act only supplements the requirements, for example in Section 23 (1) In the context of processing operations within the processor's scope of activity, the data subject may seek judicial remedy against the controller or the processor if he considers that the controller or the processor acting on behalf of, or instructed by, the controller infringes, in the course of processing his personal data, the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data. (2) The controller or the processor shall be obliged to prove that the processing complies with the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data, in particular with the fundamental requirements specified in section 4 (1) to (4a) in the case of processing operations under section 2 (3).

Section 25/E governs the duty of the data controller to keep records and logbook of its activities either as a controller or a processor.

(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 Privacy Act follows the provisions of the GDPR in this respect, there are no specific requirements for data processing in research.

13.2 Commercialization of data

13.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Act CXIX of 1995 on the use of name and address information serving the purposes of research and direct marketing	https://net.jogtar.hu/jogszabaly?docid=99500119.TV	Hard law (act of Parliament)	The scope of this Act includes the natural and legal persons, and the organisations without legal entity, requesting or using name and address information for the purpose of establishing contact for scientific research, public opinion survey, market research and direct marketing reasons. The scope of this Act shall not be extended to research activities conducted in accordance with Act LXVI of 1995 on the Protection of Public Documents, Public Archives and Private Archive Materials
***Act CVIII of 2001* on certain issues of electronic commerce services and information society services**	https://net.jogtar.hu/jogszabaly?docid=a0100108.tv	Hard law (act of Parliament)	The provisions of this Act shall apply to: a) information society services provided from the territory of the Republic of Hungary or targeting the territory of the Republic of Hungary; b) natural and legal persons and organisations without legal personality considered to be recipients of the services or service providers in respect of the services identified in

			subparagraph a). (2)2 Service providers established in the territory of other Member States to the Agreement on the European Economic Area and providing services targeting the Republic of Hungary shall not be subject to the requirements pertaining to the coordinated field. (3) This Act shall not be applied to the information society services provided and used in court or other official proceedings and shall be without prejudice to legal acts on the protection of personal data. (4)3 This Act shall not be applied to private communications specified herein.
Act LXXVI of 1999 on copyright	https://www.hipo.gov.hu/English/jogforras/hungarian_copyright_act.pdf	Hard law (act of Parliament)	(1) This Act shall protect literary, scientific and artistic creations. (2) All literary, scientific and artistic creations are protected by copyright, regardless of whether or not they are specified in this Act. Such creations are, in particular: p) databases qualifying as collection of works.
Act LXIII of 2012 on the reuse of public sector information	https://ec.europa.eu/digital-single-market/en/news/2012-évi-lxiii-törvénya-közadatok-újrahasznos%C3%ADtásáról-hungarian-act-lxiii-2012-re-use-public	Hard law (act of Parliament)	Implements EU directives 2003/98/EC and 2013/37/EU

Main regulatory tools addressing data commercialization in Hungary.

13.2.2 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)?

National legislation does not prohibit such contracts.

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

Yes.

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

No.

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

Such secondary use is regulated only in the case of public sector information (PSI).

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

No

13.2.3 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?

None of the above theoretical approaches can be derived from acts of Parliament. Decisions of the Constitutional Court are based on the theory of informational self-determination, very much like those of the German CC, linking the right to data protection to individual dignity and the general personality right.

(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?

Act LXXVI of 1999 on copyright regulates the protection of databases keeping in mind that according to paragraph 3 of Section 60/A the provisions relating to databases shall not apply to software used for the creation or operation of databases having contents accessible by computer devices. As a background legislation the Civil Code is applicable.

As to the value of the data, direct marketers or researchers can obtain personal data from the citizen registry maintained by the Ministry of Interior. In the framework of the so called "group data access", data of persons in a certain group (age, marital status, etc) can be obtained. The fee for such queries can be interpreted as "value" of the data; it depends on the media the data transferred on, the key data of the query, etc. For the table of the fees, see https://nyilvantarto.hu/letoltes/adatszolgaltatas_csoportos_dijai.pdf.

13.3 Security and cybersecurity

13.3.1 General Regulatory Framework

Regulation	Type of regulation	Brief description and scope
Act L. of 2013 on the electronic information security of state and municipal organization	Act Hard law	In the context of cyber security, information security is treated as an organizational requirement and cyber security perceived as an inter-organisational issue, thus the duty of

		state organs. This perception is reflected in the national legislation on cyber security. Act L of 2013 on the electronic information security of state and municipal organization and Hungary's National Cybersecurity Strategy deal with the cyber defence structure. a cyber defence centre in Hungary, namely a Cyber Security Centre. The government built up a centralized IT operation and development company in the past few years called NISZ Zrt. (National Info Communication Service Provider and its subsidiaries) which has a central role. The operation of the National Telecommunication Core Network's (NTG) network security is being operated by the NISZ as of summer of 2013 – in close cooperation with the newly established Government Incident Response Team (Gov-CERT – Hungary). The Act set up the National Electronic Information Security Authority under the Ministry of National Development. As a specialized authority, National Security Authority is involved in their activities with forensic log analysis and vulnerability testing. The existing Government Computer Emergency Response Team (GovCERT) responsibilities have been migrated to the Special Service for National Security. According to Section 23, the National University of Public Service developed training for those responsible for the security of electronic information systems and staff organizations.
187/2015. (VII. 13) Government Decree on the cooperation arrangement between application service providers ensuring encrypted communication and organisations entitled to carry out secret information gathering	Government Decree Hard law	The National Cyber Defence Institute formed in the Special Service for National Security with the following elements: • administration by National Electronic Information Security Authority • incident management and response by GovCERT-Hungary • forensic log analysis and vulnerability testing by National Security Authority This is also the actual setup as of January 2018. National Cyber Defence Institute was competent national authority according to NIS Directive. There are four designated CSIRTs: LRLIBEK for critical infrastructures, operated by National Directorate General for Disaster

		Management, Ministry of the Interior, MILCERT operated by the Military National Security Service, Hun-CERT the Hungarian Computer Emergency Response Team for Council of Internet Service Providers operated by the Hungarian Academy of Sciences Institute for Computer Science and Control, and NIIF-CSIRT, which is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academical research organisations and non-profit institutions in Hungary operated by National Information Infrastructure Development Institute.
Government decree No. 271/2018 on the tasks and powers of incident handling centres, and laying down rules for the handling and technical investigation of security incidents and the conduct of vulnerability assessments	Government Decree Hard law	
Government decree No. 270/2018 on the supervision of electronic information security of services related to information society, and the procedure for security incidents	Government Decree Hard law	
Decree of the Ministry of Interior 41/2015 on the Technology Security and Secure Information Tools and Products, further the Requirements for Assigning in Security Units and Security Levels Established in Act L of 2013 on the Electronic Information Security of State and Municipal Bodies	Decree of the Ministry of Interior Hard law	

13.3.2 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 legislator follows the strategy for the implementation of the directive, the majority of modifications of acts has been completed, the adjustment of the organizational structure and coordination is under way, international cooperation has been strengthened, establishing of taking common responsibilities of the private and public spheres is necessary, educational and research programmes have to be encouraged, awareness raising and the protection of children have to be strengthened.

(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?

Yes, Section 22 of Act L of 2013 regulates data protection related requirements for the defence of electronic information systems under the scope of the Act.

13.3.3 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?

Section 25/J and Section 25/K of the Privacy Act regulate this area in detail:

(1) The controller or the processor acting on behalf of, or instructed by, the controller shall record the data according to paragraph (5) a), c) and d) connected to any personal data breach occurring in relation to the data processed by it, and it shall, without undue delay but not later than within seventy-two hours after having become aware of it, notify the personal data breach to the Authority. (2) The personal data breach should not be notified when it is unlikely to result in a risk to the enforcement of the data subjects' rights. (3) If the controller is prevented from performing in due time its obligation of notification according to paragraph (1), it shall perform the notification without delay after the obstacle ceases to exist, together with attaching to the notification its statement on the reasons for the delay. (4) If the personal data breach occurred in the context of the processor's activity, or if the personal data breach is otherwise detected by the processor, it shall notify the controller of the personal data breach without delay upon becoming aware of it. (5) In the framework of the obligation of notification under paragraph (1), the controller shall a) describe the nature of the personal data breach, including, where possible, the scope and approximate number of data subjects concerned, as well as the scope and approximate number of personal data records concerned, b) communicate the name and contact details of the data protection officer or other contact point designated to provide more information, c) describe the likely consequences of the personal data breach, and d) describe the measures taken or proposed to be taken by the controller to address the personal data breach for mitigating the possible adverse effects resulting from the personal data breach and for other purposes. (6) If any of the information specified in paragraph (5) a) to d) is not at the disposal of the controller at the time of making the notification, the controller shall supplement such data subsequently, without delay, after becoming aware of the availability of the information. (7) If the personal data breach

affects any data transferred to the controller by the controller of another EEA State, or transferred by the controller to the controller of another EEA State, the information specified in paragraph (5) shall be communicated without delay by the controller to the controller of that EEA State. (8) With the exception of the notifications pertaining to classified data, the obligation of notification specified in paragraph (1) shall be performed by the controller through the electronic platform provided for this purpose by the Authority. (9) With regard to processing for national security purposes, the provisions of paragraphs (1) to (8) shall be applied, with the derogation that if the performance of the controller's obligation of notification under paragraph (1) and the obligation of communication under paragraph (7) is in conflict with the interests of national security, they shall only be performed after such interests of national security have ceased.

Section 25/K (1) When the personal data breach is likely to result in consequences materially influencing the enforcement of a fundamental right of the data subject (hereinafter "high-risk personal data breach"), the controller shall, with the exception of processing for national security purposes, communicate the personal data breach to the data subject without delay. (2) The controller shall be exempted from the obligation of informing the data subject according to paragraph (1) if a) the controller had implemented appropriate technical and organisational protection measures before the personal data breach, and those measures were applied to the personal data affected by the personal data breach, in particular those, such as encryption, that render the personal data unintelligible to any person who is not authorised to access them, b) after having become aware of the personal data breach, the controller has taken subsequent measures that ensure that the consequences materially influencing the enforcement of a fundamental right of the data subject are not likely to occur, c) informing the data subject directly according to paragraph (1) requires disproportionate efforts by the controller, and therefore the controller provides the data subjects with adequate information on the personal data breach by way of public communication accessible to anyone, or d) communication is excluded by an Act according to the provisions of paragraph (6). (3) In the framework of the obligation of communication under paragraph (1), the controller shall present the nature of the personal data breach and it shall provide the data subject with the information specified in section 25/J (5) b), c) and d). (4) When, on the basis of the notification performed according to section 25/J (1), the Authority establishes that it is necessary to inform the data subject due to the high risk of processing, the controller shall implement any outstanding obligation of communication under paragraph (1) without delay after the establishment of this obligation. (5) The controller shall not be obliged to perform the obligation of communication according to paragraph (1) if, on the basis of the notification performed under section 25/J (1), the Authority has established the existence of a circumstance specified in paragraph (2) a) to d). (6) By way of derogation from the provisions under paragraphs (1) to (5), an Act may exclude, restrict or require the delayed performance of providing the data subject with information, on the conditions and for the reasons specified in section 16.

Sections 19-20 of the Act L of 2013 regulates the procedure to be followed in the case of a security incident and the procedure of the incident handling unit that performs the following tasks: management of security incidents, threat management, duty service, analysis / assessment, cyber security exercise, training, raising awareness, support of the identification of the responsible person, vulnerability assessment, cooperation with Internet Service Providers in case of management of security incidents, to inform regularly the Management, security management and vulnerability assessment unit,

vulnerability assessment, Investigation of security incidents, perform tasks in connection with information security in the EMIR/FAIR systems.

13.3.4 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 National Cyber Defence Institute formed in the Special Service for National Security with the following elements: administration by National Electronic Information Security Authority, incident management and response by GovCERT-Hungary, forensic log analysis and vulnerability testing by National Security Authority. This is also the actual setup as of January 2018. National Cyber Defence Institute was competent national authority according to NIS Directive.

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

No such issues are regulated in specific legislation, the Civil Code is applicable

13.4 Enforcement: fines and sanctions

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

Act C of 2012 on the Criminal Code7 (hereinafter referred to as the Criminal Code) defines the misuse of personal data as a criminal offense in Section 219: that (1) any person who, in violation of the statutory provisions governing the protection and processing of personal data: a) is engaged in the unauthorized and inappropriate processing of personal data; or b) fails to take measures to ensure the security of data is guilty of a misdemeanour punishable by imprisonment not exceeding one year. (2) The penalty in accordance with Subsection (1) above shall also be imposed upon any person who, in violation of the statutory provisions governing the protection and processing of personal data, fails to notify the data subject as required, and thereby imposes significant injury to the interests of another person or persons. (3) Any misuse of personal data shall be punishable by imprisonment not exceeding two years if committed in connection with special data. (4) The penalty shall be imprisonment not exceeding three years for a felony if the misuse of personal data is committed by a public official or in the course of discharging a public duty.

The criminal offense of the breach of information systems or data is regulated in Section 423 of the Criminal Code. (1) Any person who: a) gains unauthorized entry to an information system by compromising or defrauding the integrity of the technical means designed to protect the information system, or overrides or infringes his user privileges; b) disrupts the use of the information system unlawfully or by way of breaching his user privileges; or c) alters or deletes, or renders inaccessible without permission, or by way of

breaching his user privileges, data in the information system is guilty of a misdemeanour punishable by imprisonment not exceeding two years. (2) The penalty shall be imprisonment between one to five years for a felony if the acts defined in Paragraphs b)-c) of Subsection (1) involve a substantial number of information systems. (3) The penalty shall be imprisonment between two to eight years if the criminal offense is committed against works of public concern. (4) In the application of this Section 'data' shall mean facts, information or datum stored, controlled, processed and transmitted in information systems in all forms which allows them to be processed in information systems, including those programs designed to execute certain functions by the information systems. Compromising or defrauding the integrity of the computer protection system or device as another possible offense is regulated in Section 424 of the Criminal Code. (1) Any person who, for the commission of the criminal offense defined in Section 375 or 423: a) creates, transfers, supplies, obtains or places on the market passwords or computer programs required therefor or facilitating thereof; or b) offers his economic, technical and/or organizational expertise to another person for the creation of passwords or computer programs required therefor or facilitating thereof is guilty of a misdemeanour punishable by imprisonment not exceeding two years. (2) In the case of Paragraph a) of Subsection (1), any person who confesses to the authorities his involvement in the creation of any password or computer program required for the commission of the criminal offense, or facilitating thereof, before the authorities learned of such activities through their own efforts, and if the person surrenders such produced things to the authorities and assists in the efforts to identify the other persons involved, shall not be prosecuted. (3) For the purposes of this Section 'password' shall mean any identifier comprised of a string of alphanumeric characters, codes, biometric data or the combination thereof, designed to gain entry into an information system or any segment thereof.

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

According to Section 60 of the Privacy Act paragraph (3) the Authority shall commence an authority procedure for data protection ex officio if a) it finds on the basis of its inquiry that an infringement related to the processing of personal data has occurred or there is an imminent threat of such an infringement, and, after the notification issued or the recommendation presented in accordance with section 56, the infringement has not been remedied or its imminent threat has not been eliminated within the time limit specified by the Authority, b) it finds on the basis of its inquiry that an infringement related to the processing of personal data has occurred or there is an imminent threat of such an infringement, and a fine may be imposed according to the provisions of the General Data Protection Regulation.

In Section 61 paragraph (1) In its decision adopted in authority procedures for data protection, the Authority bg) may impose a fine, (4) The amount of the fine shall be between one hundred thousand and twenty million forints if the fine is imposed a) pursuant to paragraph (1) b) bg), or b) pursuant to Article 83 of the General Data Protection Regulation and the party required to pay the fine imposed in a decision adopted in accordance with an authority procedure for data protection is a budgetary organ. (5) In deciding whether it is justified to impose a fine pursuant to paragraph (1) b) bg), and in determining the amount of the fine, the Authority shall take all circumstances of the case into account, in particular the number of data subjects affected by the infringement, the gravity of the infringement, the fault, and whether the infringing party was previously found to have committed an infringement concerning the processing of personal data.

Act L of 2013 and Government Decree 187/2015 regulates that a fine is imposed in the capacity of the National Electronic Information Security Authority responsible for the supervision of information security within the scope of these pieces of legislation, if the organisation concerned does not comply with security requirements set down in the regulations, and other related procedural rules.

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

Data protection offences referred to above are offences to be prosecuted ex officio

13.5 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?

The Data Protection Authority provided an assessment tool for DPIAs which is available on this site: https://www.naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html

Information security: the GovCERT.HU website: http://tech.cert-hungary.hu/ provides information about services, incident reporting and announcements, .e.g. http://tech.cert-hungary.hu/.

No other tools or guidelines are promoted that we know of.

(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?

Government Decree 13/2011. (II. 22.) sets out the rules for exporting dual use technologies. Government offices („kormányhivatal") are responsible for issuing national permits for export.

National Cyber Defence Institute, described above, provides enterprises advice on IT security issues on its webpage.