'Big data analytics' and processing of health data for scientific research purposes : The Hungarian legal framework

Research Protocol by András Jóri, Andrea Soós and Katalin Horváth-Egri,
in Budapest, Hungary, 21 August 2018

Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

1. Overview of the legal framework

a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018)

What are the relevant applicable provisions governing the processing of health data in your country? Please provide online references (also to an English version, if available), a brief description and any specific relevant information.

- **THE PRIVACY ACT**

In Hungary fundamental rules regulating data protection are set down in the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information[1] (hereinafter referred to as: the Privacy Act). Data protection has been regulated since 1992, when the first data protection act was adopted. It was later amended a number of times, but significantly in 2003 and 2005, to ensure the proper harmonisation of the provisions of the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[2]. The Privacy Act will be amended to the necessary extent to enable the compliance with the General Data protection Regulation (hereinafter: GDPR) possibly in 2018. The specialty of the Privacy Act is that regulations covering implementation of the constitutional right to freedom of information is incorporated in the same act for enforcing of the rights to access and disseminate data of public interest and data public on grounds of public interest.

The Privacy Act lays down the fundamental rules for data processing activities with a view to ensuring that the right to privacy of natural persons is respected by data controllers. Principles of data protection based on the European data protection law govern the Hungarian legislation that are applicable throughout all the processing activities related to personal data.

Basic concepts of the Privacy Act relevant to the purposes of this study are as follows:

Personal data shall mean data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject.

Special data (also known as sensitive data) shall mean:

[1] https://naih.hu/files/Act-CXII-of-2011_EN_15.11.2016-003-.pdf

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

a) personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life,

b) personal data concerning health, pathological addictions, or criminal record.

Data processing shall mean any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans).

Processing personal data relating to scientific research (Section 12)

(1) Personal data recorded for scientific reasons must be used only for scientific research projects.

(2) Personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can be attributed to an identified or identifiable natural person shall be stored separately. Such data may be linked to other data if it is necessary for the purposes of research.

(3) An organization or person conducting scientific research shall be allowed to disseminate personal data only if:

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Section 21 regulates the data subject's right to object to the processing of data relating to him, in particular if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research (point b) and c)) in all other cases prescribed by law.

Furthermore the Data Protection Authority's data protection register shall not cover operations if it serves the purposes of scientific research.

- **ACT ON THE USE OF NAME AND ADDRESS INFORMATION SERVING THE PURPOSES OF RESEARCH AND DIRECT MARKETING**

In respect of scientific research Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing[3] further 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 this 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 research oriented 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 of research oriented data use must be kept on file in order to provide proof of

[3] http://www.ceecprivacy.org/htm/dmtv-en.htm

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the legitimacy of the data use and for inspection until the use of the data is terminated. (3) 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.

- **THE ACT ON HEALTH**

The Act CLXV of 1997 on Health[4] (hereinafter referred to as: the Act on Health) defines the main objectives and purposes in general, i.e. to foster the improvement of health of the individual, and thereby, of the population, by determining the system of conditions and means influencing health, as well as the responsibilities of those involved in the establishment thereof, to contribute to ensuring equal access to health care services for all members of society, to create the conditions whereby all patients may preserve their human dignity and identity and their right of self-determination and all other rights may remain unimpaired. The right to information prevails in the processing activities of personal data, the practicing of which is a prerequisite for applying adequately the right to self-determination. A patient's personal freedom and right of self-determination can be restricted exclusively in cases and in a manner justified by his/her health status and defined in this Act. As a general background legislation, the Act on Health regulates the content of the health care documentation, the requirements and basic provisions (including the detailed rules of providing information to the data subjects, practicing data subjects' rights) for the retaining of medical documentation, the health and medical records. Section 24 regulates the right of access of the data subject to the health care documentation.

- **THE MEDICAL DATA ACT**

The Act XLVII of 1997 on the Processing and Protection of Health Care Data and Related Personal Data[5] (hereinafter referred to as: Medical Data Act) aims to regulate the terms and objectives of the processing of special data concerning health and related personal data. The Medical Data Act protects the rights of the data subjects from the unauthorized access to their personal data. It specifically defines the scope of personal data, the purposes for which the data may be collected, it regulates the scope of entities, persons entitled for the accessing and controlling of data concerning health. Data subjects rights, such as right to information, access to information, rectification, objection, are provided for in a detailed manner in the Medical Data Act. In respect of the legal authorization for the data processing, it may be important to note that the recording or providing of personal data concerning health is regarded as part of the medical treatment. Providing of personal data concerning health and identifying data by the data subject is voluntary.

Section 21 of the Medical Data Act regulates data processing for the purposes of scientific research. It lays down that (1) for the purposes of scientific research the data may be inspected with the permission of the head or the data protection officer of the health institution, however, the respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. In the course of scientific research, no copy can be made on stored data which contains personal identifying information. (2) The individuals who had access to the stored data pursuant to paragraph (1), as well as the purpose and date of inspection shall be recorded. Such records shall be retained for 10 years. (3) The refusal of the research application shall be justified by the head or the data protection officer of the organization. In case of the refusal of the application the applicant may bring the case to the court. For bringing an action and carrying out the procedure the

[4] http://www.patientsrights.hu/dokumentumletoltes.php?tip=letoltesek_eng&kod=1&file=1997_cliv_tv_eng.pdf

[5] https://net.jogtar.hu/jogszabaly?docid=99700047.TV

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

rules regulating the procedure that may be brought in case of the refusal of the request for access to public information of the Privacy Act are applicable.

For the protection of the personality rights of the patient all health service providers have to make efforts to provide anonymized, group data provision for scientific purposes - also by complying with other legal requirements - in order the personal data entrusted with him primarily for the purposes of medical treatment will not be accessed by external third parties. Such medical researches may only be commenced after the test of ethical conformity, in possession of the approved research plan.

Shared electronic health records are indirectly relevant in this context because they can potentially be an important source for health-related research.

- **ELECTRONIC HEALTH COOPERATION SERVICE SPACE**

The Electronic Health Cooperation Service Space (hereinafter referred to as EESZT – Elektronikus Egészségügyi Szolgáltatási Tér) was established by the medical data Act, and the relevant provisions thereof are applicable as of 1st June 2016.

Pursuant to the Medical Data Act EESZT qualifies as data controller in cases of the central event catalogue, health profile, records of self-determination, electronic referral and digital image transmitting services. For the sufficient operation of these services the processing of personal data of patients is essential. These data processing activities are in compliance with the current data controlling system of the Medical Data Act, and in all cases the data processing can be performed in line with the purposes of data processing set down in the Medical Data Act.

In respect of data protection it is an element of guarantee relating to the use of the system that a single record of identification and access management is to be kept for the purposes of controlling of the identification of users involved in the treatment, and ensuring the legality of data processing by means of the EESZT. This record contains the users of the EESZT, and the patient may limit the scope of those entitled to access his/her data by making a statement in the records of self-determination.

Further detailed rules are defined in **the 39/2016. (XII. 21.) decree** on specific rules regarding the Electronic Health Cooperation Service Space[6]. The data controller and the data processor may process health data only by keeping professional secrets. The EESZT provides for that all personal data stored in it may be accessed by doctors. The operation of this medical cooperation service space in compliance with the requirements of data protection and safety is ensured by guarantees, such as preliminary privacy impact assessment, applying criminal legal consequences if necessary, appointing a data protection officer, follow-up checks, and citizen control by using the records of self-determination.

- **CRIMINAL CODE**

Act C of 2012 on the Criminal Code[7] (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

[6] https://net.jogtar.hu/jogszabaly?docid=A1600039.EMM&timeshift=fffffff4&txtreferer=00000001.TXT

[7] http://thb.kormany.hu/download/a/46/11000/Btk_EN.pdf

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

personal data; or b) fails to take measures to ensure the security of data is guilty of a misdemeanor 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.

Considering that most of health data have been controlled and/or processed by means of electronic devices and information systems, in particular via the EESZT, the criminal offense of the breach of information systems or data is worth special attention 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.

b. Revision of the current legal framework under the GDPR

How are the necessary changes to the national data protection framework introduced by the GDPR addressed in your country? What is the adopted legislative approach?

Is the GDPR implemented in your country by an entirely new legislative text or via amendments to the current data protection law? Please explain.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Ministry of Justice made available for public consultation its proposal of the draft of the amendments of the Privacy Act. The objective of the proposal is to ensure the compliance of the national data protection legislation with the provisions of the GDPR[8] on 29th August 2017. Although the GDPR is directly applicable, the amendment of relevant parts the Privacy Act, and the amendment of numerous sector specific legislation is necessary as well.

The National Data Protection Authority was involved and consulted in the procedure that focused on the possible amendments of the Privacy Act. The DPA provided to the legislator its opinions a number of times regarding the necessary changes in the text[9][10][11], and the status of the Authority[12]since the absolute majority of votes of representatives of the Parliament is required for the setting up of the Data Protection Authority in conformity with the GDPR, and the legislation related to imposing fines and associated tax rules[13].

According to the known text of the draft of the Privacy Act, it implements the provisions of the Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data.

The Privacy Act was amended by the Act XXXVII of 2018 on amending the Act CXII of 2011 on Informational Self-Determination and Freedom of Information in connection with the reform of data protection in the European Union, and on amending other related laws[14] on 24 July 2018; the provisions are in effect as of 25 July 2018.

The amended Privacy Act makes a reference for GDPR for the processing activities under the scope of the Regulation, while sets out detailed regulation implementing the Police Directive. In some cases, the Hungarian lawmaker makes use of the opening clauses of GDPR, e.g. sets out rules for enforcement of rights under GDPR for the personal data of deceased data subjects (rights can be enforced by a mandated person, for a five-year period following the date of the death). The concepts of health data, genetic data and biometric data, following the respective definitions of GDPR also appear in the text (however, these are relevant only for the implementation of the Police Directive, otherwise the definitions of GDPR are to be applied directly).

Processing data for the purpose of scientific or any other research is not regulated by the amendment, in general, the relevant and appropriate rules may be applicable that are connected to the specific case. Sector specific regulation is intended to set out the relevant requirements in particular relation to the processing of health data for

[8]http://www.kormany.hu/download/d/88/21000/20170828%20Előterjesztés%20az%20információs%20önrendelkezési%20jogról%20és%20az%20információszabadságról%20szóló%20törvény%20jogharmonizációs%20célú%20módos%C3%ADtásáról.zip#!DocumentBrowse

[9]https://naih.hu/files/NAIH-244-13-2017-J-170911.pdf

[10] https://naih.hu/files/NAIH-244-14-2017-J-170921.pdf

[11]https://naih.hu/files/NAIH-244-15-2017-J-170925.pdf

[12]https://naih.hu/files/NAIH-579-3-2018-J-180122.pdf

[13]https://naih.hu/files/NAIH-579-2-2018-J-180122.pdf

[14]https://net.jogtar.hu/jogszabaly?docid=A1800038.TV&timeshift=fffffff4&txtreferer=00000001.TXT

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the purpose of scientific research. However, the related sector-specific legislation has not yet been proposed or adopted.

c. The national data processing authority

Can you provide a short description of the role of the data protection supervisory authority in your country in the domain of processing health data for research purposes under the current legal framework?

The National Authority for Data Protection and Freedom of Information (hereinafter referred to as: the Authority) is responsible for supervising and defending the right to the protection of personal data and to freedom of information in Hungary. Its responsibilities extend to cover both the state and private sectors.

The Privacy Act does not provide for the separate consideration of the processing health data for research purposes for the Authority, it investigates complaints or draft legislation on the same basis, the same rules apply in relation to the role of the Authority.

According to the Privacy Act, the Authority is an autonomous administrative organ. The Authority is an independent body that is subject to Hungarian law only, it may not be instructed in its official capacity, shall operate independent of any outside interference, without any bias. Tasks may only be prescribed for the Authority by acts of Parliament.[15] The Authority is a central budgetary organ with the powers of a budgetary chapter, and its budget shall constitute an independent title within the budgetary chapter of Parliament.[16]

The Privacy Act is comprehensive in scope, and concerns all data control and data processing activities undertaken in Hungary. The Privacy Act defines these activities as those which relate to the data of a natural person, as well as data in the public interest and data made public on the grounds of being in the public interest. Compared to the former system, the new regulations confer the Authority with broader competency to pursue violations of both informational rights. In particular: anyone is entitled to request an investigation from the Authority on the grounds of infringement of data protection law. The Authority is entitled to launch an official data protection procedure if it is presumed that the illegal processing of personal data concerns a wide scope of persons; concerns special data, or significantly harms interests or results in the risk of damages. The Authority may decide to order the correction of inauthentic personal data; order the blocking, deletion or destruction of illegally controlled personal data; prohibit the illegal control or processing of the personal data; prohibit the transfer of the personal data to other countries; order notification of the data subject, should the controller have unlawfully refused to do so; f) impose a fine ranging from 100,000 HUF to 10,000,000 HUF; g) order the disclosure of their decision in the interest of data protection or to protect the rights of a greater number of data subjects. The Authority registers data processing undertaken in respect to personal data in a data protection file or registry in order to facilitate access to information for the data subject. The Authority is authorised to launch a confidentiality review procedure, should, pursuant to information received, it may be presumed that national classified information has been illegally classified. The Authority provides

[15] Section 38 of the Privacy Act

[16] Section 39 of the Privacy Act

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

a data protection audit as a service to those entities that request it. This audit is designed to provide a high standard of data protection and security relating to data processing operations.

Sections 52-58. of the Privacy Act regulate the procedure of the Authority on investigations, Sections 60-61. of the Privacy Act regulates the administrative proceedings for data protection of the Authority. These procedures may be applicable in cases of scientific researches, as well, the Act specifies only the administrative proceedings for the control of classified data in Sections 62-63.

Can you describe the adopted or proposed changes to this role of the national data protection authority to ensure compliance with the GDPR?

According to Article 54 of the GDPR the Member State must set in law the rules establishing the supervisory authority. In Hungary the relevant amendment of the legislation to establish the supervisory authority requires the absolute majority of voting representatives of Parliament, it has not happened yet.

The draft amendment of the Privacy Act incorporates references to the GDPR and, where necessary, the legislation is detailed. The competence and the scope of proceedings of the Authority will be widened: dealing with data protection incidents, data protection impact assessment, prior consultation, authorization and advisory powers, approving codes of conduct, certification mechanisms, all other tasks regulated in the GDPR (Article 57 of the GDPR) but not included in the draft legislation, and participation in the cooperation procedure.

2. Transposition of Article 8.4 of Directive 95/46

Did your national legislator insert any additional exemptions for the processing of health data for research purposes? How is it/are they formulated? Please explain. Are there additional exemptions issued by the DPA?

Art. 8.4 of Directive 95/46: “4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.”

a. Transposition of Article 8.4 of Directive 95/46

What are the exceptions to the prohibition of processing sensitive data? Do any of these exceptions address scientific research in the field of health?

The Authority may not lay down or authorize or approve by decision any exemptions from in addition to those laid down in paragraph 2 of Article 8 of Directive 95/46.

Section 2 of the Privacy Act defines personal data: data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological,

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject. Section 3 of the Privacy Act defines special data, and its paragraph b) specifies health data: personal data concerning health, pathological addictions.

Sections 5 and 6 lay down rules for the legal authorisation for data processing of any kind, and in particular for the processing of special data. According to Section 5 of the Privacy Act special data may be processed according to Section 6, and under the following circumstances: a) when the data subject has given his consent in writing, or

b) when processing is necessary for the implementation of an international agreement promulgated by an act concerning the data under Point 3.a) of Section 3, or if prescribed by law in connection with the enforcement of fundamental rights afforded by the Fundamental Law, or for reasons of national security or national defence, or law enforcement purposes for the prevention or prosecution of criminal activities, or

c) when processing is necessary for the performance of a task carried out in the public interest concerning the data under Point 3.b) of Section 3.

(3) Where data processing is mandatory, the type of data, the purpose and the conditions of processing, access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or municipal decree in which it is ordered."4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

The Privacy Act generally regulates the processing, or rather inspecting health data for the purposes of scientific research and the Medical Data Act regulates some exemptions by specifying purposes of the data controlling, and the permitting procedure of the processing of health data for the purposes of scientific research.

According to point a) of Section 3 of the Medical data Act the definition of health data is more specific, it means data on the patient's physical, mental and emotional condition, addiction, the circumstance of illness and death, the cause of death, and any other data associated with the above (e.g. behaviour, environment, occupation). This definition implies that the definition of health data is not restricted to medical information. Pursuant to paragraph 1 of Section 9, the Medical Data Act the patients' health data are collected by the competent healthcare providers, as part of the medical treatment. It is up to the healthcare professional to decide on the type of health data to be collected.

The processing of health data may be performed for different purposes defined in two separable groups of the Medical Data Act. The first group of purposes for the controlling of data includes the purposes of the healthcare system: the patients' health and personal data should primarily be used for: health prevention, health amelioration and maintenance, medical treatment, following the medical pathway of patients, public health and infection prevention purposes, and enforcing patients' rights (paragraph 1 of Section 4 of the Medical Data Act). The other group of purposes contains the purposes of the controlling performed by other organs (points a)-t) of paragraph 2 of Section 4 of the Medical Data Act). The purposes referred to under Section 4 provide for the first and secondary use of data. Rules applicable to the secondary use of data are regulated in paragraphs 2-3 of Section 4 of the Medical data Act.

Section 21 of the Medical Data Act regulates data processing for the purposes of scientific research. It lays down that (1) for the purposes of scientific research the data may be inspected with the permission of the head or the data protection officer of the health institution, however, the respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. In the course of

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

scientific research, no copy can be made on stored data which contains personal identifying information. (2) The individuals who had access to the stored data pursuant to paragraph (1), as well as the purpose and date of inspection shall be recorded. Such records shall be retained for 10 years. (3) The refusal of the research application shall be justified by the head or the data protection officer of the organization. In case of the refusal of the application the applicant may bring the case to the court. For bringing an action and carrying out the procedure the rules regulating the procedure that may be brought in case of the refusal of the request for access to public information of the Privacy Act are applicable.

b. The regime applying to the processing of personal data for health research purposes

Is there a specific regime applying to data processing for research in the field of health purposes?

Although there are specific provisions regulating, for instance, biomedical research involving human subjects in Chapter VIII of the Act on Health, the relevant legislation concerning data protection does not differentiate if processing of personal data for research in the field of health purposes is involved.

Section 21 of the Medical Data Act, as quoted above, regulates data processing for the purposes of scientific research without making differences of the subject of the research. It lays down that for the purposes of scientific research the data may be inspected *with the permission of the head or the data protection officer of the health institution.*

The Medical Data Act regulates the use of health data in a way that its regulations are applicable to any person carrying out scientific work.

Decree 23/2002. (V. 9.) of the Ministry of Health on biomedical research involving human subjects[17] 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.

Decree 35/2005 (VIII. 26.) of the Minister of Health on the clinical trial and application of correct clinical practices of investigational medicinal products intended for use in humans[18] ensures the procedural guarantees of the aforementioned researches, in compliance with the provisions of the Privacy Act and the Medical Data Act, it ensures that the examination cannot be commenced without the prior written and informed consent of the individual, it ensures both the protection of individuals and their personal data, it provides for the rights of the data subjects and details the procedure of the official authorization of the research. Section 4 of the Decree regulates that the subject's rights, safety and wellbeing are given priority over the interests of science and society, therefore, risks affecting research subjects must be minimised. Pursuant to paragraph 8 of Section 5 clinical trials shall be governed by the provisions of the Privacy Act, the Medical Data Act, and in different legislation on data processing. The provisions on

[17] https://net.jogtar.hu/jogszabaly?docid=a0200023.eum

[18] http://www.mkvt.hu/PDF/decree35.pdf

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the retention of trial documentation contain specific regulations in Section 24, laying down that the trial's master dossier must contain every basic document allowing for both the continuation of the clinical trial and the assessment of data quality. The documents must show whether the investigators and the sponsor complied with the GCP principles. The trial's master dossier serves as the basis for inspections performed by an inspector independent from the sponsor or by the authorities. Any change in the ownership of processed data and the trial documentation must be documented. The new owner must make a written statement on agreement with the compliance with provisions governing data processing and archiving.

From which generally applicable data protection provisions are researchers exempted and under what conditions?

The above written is applicable here. As general background legislation, Section 12 of the Privacy Act sets down that personal data recorded for scientific reasons must be used only for scientific research projects. Personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can be attributed to an identified or identifiable natural person shall be stored separately. Such data may be linked to other data if it is necessary for the purposes of research. An organization or person conducting scientific research shall be allowed to disseminate personal data only if:

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Section 21 of the Privacy Act regulates the data subject's right to object to the processing of data relating to him, in particular if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research (point b) and c)) in all other cases prescribed by law.

More specific requirements are regulated in Section 21 of the Medical Data Act saying that data processing for the purposes of scientific research. It lays down that (1) for the purposes of scientific research the data may be inspected with the permission of the head or the data protection officer of the health institution, however, the respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. In the course of scientific research, no copy can be made on stored data which contains personal identifying information. (2) The individuals who had access to the stored data pursuant to paragraph (1), as well as the purpose and date of inspection shall be recorded. Such records shall be retained for 10 years. (3) The refusal of the research application shall be justified by the head or the data protection officer of the organization. In case of the refusal of the application the applicant may bring the case to the court. For bringing an action and carrying out the procedure the rules regulating the procedure that may be brought in case of the refusal of the request for access to public information of the Privacy Act are applicable.

For the protection of the personality rights of the patient all health service providers have to make efforts to provide anonymized, group data provision for scientific purposes - also by complying with other legal requirements - in order the personal data entrusted with him primarily for the purposes of medical treatment will not be accessed by external third parties. Such medical researches may only be commenced after the test of ethical conformity, in possession of the approved research plan.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Authority's data protection register does not cover operations if it serves the purposes of scientific research, that is data processing for scientific purposes need not to be notified.

c. Are there additional specific conditions governing the processing of data for scientific research purposes?

What are the suitable safeguards applied to the exemption foreseen by Article 8.4 of the Directive in your country?

The regulation on the processing of sensitive data, health data for the purposes of scientific research is an exemption from the provision of Article 8.4 of the Directive. Both the Privacy Act and the Medical Data Act contain safeguards, complying with the principles of the Directive and the Privacy Act. One of the safeguards to be mentioned is the anonymity of personal data and the preliminary permission of the institute. For the protection of the personality rights of the patient all health service providers have to make efforts to provide anonymized, group or aggregated data provision for scientific purposes - also by complying with other legal requirements - in order the personal data entrusted with him primarily for the purposes of medical treatment will not be accessed by external third parties. Such medical researches may only be commenced after the test of ethical conformity, in possession of the approved research plan.

Are there any specific provisions concerning: (i) professional secrecy, (ii) express consent for specific data, or specific provisions for (iii) deceased data subjects, or (iv) specific provisions for minors or persons subject to guardianship?

(i) **Professional secrecy**

The right to professional secrecy is regulated in Section 25 of the Act on Health (1) A patient shall have the right to have persons involved in his health care disclose his health care and personal data which they might learn in the course of delivering such care (hereinafter: 'medical secret') to those entitled thereto and to have them handle such data confidentially. (2) A patient shall have the right to make a statement as to who are to receive information on his illness and the expected outcome thereof and who are to be excluded from becoming partially or fully acquainted with his health care data. (3) The health care data of the patient concerned shall be disclosed even in the absence of his consent thereto when a) ordered by law, b) required in order to protect the lives, physical safety and health of others. (4) Health care data, the lack of which may lead to the deterioration of the patient's state of health may be disclosed to a person in charge of a patient's further nursing and continuing care, without the consent of the patient concerned. (5) A patient shall have the right to have only those persons present during the course of his examination and medical treatment whose involvement is necessary in delivering such care, furthermore those persons to whose presence he has consented, unless otherwise provided by law. (6) A patient shall have the right to have his examination and treatment take place under circumstances whereby it cannot be seen or heard by others without his consent, unless this is unavoidable due to an emergency or critical situation. (7) A patient shall have the right to name the person who may be notified of his admission to an inpatient healthcare institution and the development of his state of health, and he shall have the right to exclude any person therefrom. The inpatient healthcare institution must inform the person named by the patient of his admission and any change in his placement, as well of any significant change in the patient's state of health.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Act on Health provides rules for the obligation to maintain confidentiality in its Section 138: (1) All healthcare workers and all persons employed by a healthcare provider shall be obliged to maintain unlimited duration confidentiality regarding the health of a patient, as well as regarding all data learned while providing healthcare services, irrespectively of whether said data was provided directly by the patient, or learned through an examination/test or through treatment, or learned indirectly through medical documentation or in any other manner. (2) The requirement for confidentiality shall not cover cases in which the patient has given a release, or for which statutes specify an obligation to provide said data.

In accordance with Section 7 of the Medical Data Act, entities responsible for the controlling and processing of data are bound by rules of professional secrecy, unless the patient or his/her legal representative has provided his/her consent for the disclosing of his/her health and identification data to the competent authorities, and the disclosure of the patients' health and personal data to the competent authorities is compulsory. While registering, controlling and processing health and personal data, the provisions set out in Section 6 of the Medical data Act should be complied with. Section 6 lays down that the personal and health data of patients while being controlled and processed must be protected from negligent or intentional destruction, alteration, damage, public disclosure and unauthorised access. Pursuant to Section 8 of the Medical data Act the health service provider – except the chosen family physician of the data subject and judicial medical experts – is also bound by confidentiality against those health service providers, who did not participate in the medical examination, establishment of the diagnosis, and did not contribute to the treatment or operation, unless disclosing the data was necessary for the establishment of the diagnosis or in the interest of the further treatment of the data subject.

(ii) Express consent for specific data

The express, written consent of the data subject is necessary for almost all data processing activities concerning health and/or related scientific research if the data is collected directly from the data subject, in case of indirect collection or inspection of the data the express consent is not necessary, unless otherwise specified by law.

(iii) Specific provisions for deceased data subjects

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 Act V of 2013 on the Civil Code (hereinafter referred to as: the Civil 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.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

According to paragraph 8 of Section 16 of the Medical Data Act, the Central Office for Statistics transfers the identifiable personal data of the deceased data subject with the data content defined by law 5 days after having checked the completeness and connection of the data to the registries of epidemiology and tumour, and another group of identification data specified by law to the National Heart Attack Registry. These registries delete those data of the deceased data subject that are irrelevant to be kept there as defined by the law.

The Medical Data Act regulates who may have access to the personal data of the deceased data subject in paragraph 7 of Section 7: legal representative, next of kin and inheritor based on their written request are entitled to inspect, have access to the healthcare documentation, and receive a copy of the content.

(iv) Minors and persons subject to guardianship

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.

According to paragraph 1 of Section 2:20 of the Civil Code: the legal statements of persons of partially limited legal capacity with respect to certain types of matters specified in the court ruling shall be considered valid upon the conservator's consent. If and when a persons of partially limited legal capacity becomes competent, he shall be entitled to make his own decisions concerning the validity of his pending legal statement.

In urgent cases, or in case of incapable patients, the law (paragraph 3 of Section 12 of the Medical Data Act) assumes that the patient voluntarily turned to the health professional, thus implicitly allows for the collection of the patients' health data without their consents.

Paragraph 6 of Section 24 of the Act on Health regulates that the right to inspect the medical record of a person with no disposing capacity shall be exercised by a person as defined in paragraphs 1 and 2 of Section 16, and in cases of minors and persons with limited legal capacity the person in paragraph 1, point a) or the legal representative may have access to the documentation.

Are there specific requirements about the data subject's information or about the person from whom the data was collected?

In respect of processing personal data for purposes of health research the general rules are applicable regarding providing information to the data subject either in a preliminary manner concerning obtaining the consent for the processing, or complying with the requirement of enhancing the right of the data subject to receive information throughout the data processing. No other specific requirement is set down on the information of the data subject in the relevant legislation.

Are there specific penalties if the conditions for processing for scientific research in the field of health purposes are not respected? What do those penalties entail?

Only the data subject may initiate any proceedings against an alleged breach of the data protection rules. These proceedings may include the investigations of the Data Protection Authority, The Authority may decide to a) order

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the correction of inauthentic personal data; b) order the blocking, deletion or destruction of illegally controlled personal data; c) prohibit the illegal control or processing of the personal data; d) prohibit the transfer of the personal data to other countries; e) order notification of the data subject, should the controller have unlawfully refused to do so; f) impose a fine ranging from 100,000 HUF to 10,000,000 HUF; g) order the disclosure of their decision in the interest of data protection or to protect the rights of a greater number of data subjects. Additionally, the case may be brought in criminal court or the civil court.

d. Formalities prior to processing: the general regime under the current framework

Is there a regime requiring the fulfilment of certain conditions prior to any processing activities different from that applicable to research in the field of health? If yes, what does that regime entail?

The above mentioned regulations are applicable concerning the Privacy Act and the Medical Data Act.

3. Further processing of health data (for research purposes): the current regime

How is the notion of further processing regulated in your national framework?

In the Privacy Act there is no such definition specified like further processing of data, the act defines the concepts of data transfer in Section 3 point 11: data transfer shall mean ensuring access to the data for a third party; and disclosure in point 12: disclosure' shall mean ensuring open access to the data. Pursuant to Section 12 of the Privacy Act personal data recorded for scientific reasons must be used only for scientific research projects. Principles of data protection have to be respected throughout the processing. The obligations of the third party who would receive the personal data are identical with the obligations of the initial data controller regarding the protection of personal data.

When transferring data to other countries may occur, than Section 8 is applicable: personal data may be transmitted by a data controller covered by this Act to a data controller or processor operating in a third country, or may be transferred to a data controller or processor operating in a third country if: a) the data subject has given his explicit consent, or b) the conditions laid down in Section 5 and/or Section 6 for data processing are satisfied and - save where Subsection (2) of Section 6 applies – the adequate level of protection of the personal data have been ensured in the third country during the course of the control and processing of the data transferred. Paragraph 2 regulates when the adequate level of protection of personal data is ensured.

Are there specific conditions to the further processing for scientific research in the field of health purposes?

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Specific rules are set down in the Medical Data Act. These rules have been presented above. Hungarian legislation allows for the secondary use of health data, for instance, scientific, epidemiological, planning and evaluation purposes. Secondary use is subject to strict data protection rules based on the Medical Data Act often allowing for the use of health data without reference to the identification of patients. Regarding archiving, it is noted that Hungarian legislation provides for the controlling and processing of patient data for a limited period of time. It provides for the secondary use of health data, which includes in accordance with Sections 18-19: epidemiological examinations and analysis, the planning of medical services and the quality and performance evaluation, health data could also be used by organisations responsible for planning patient pathways. Section 20: statistical data processing, Section 21: scientific research.

Paragraph 2 of Section 18 provides that while carrying out the professional evaluations, the head of the competent organisation must make sure that the health and personal data of the patient is accompanied with a code. The code will disable the competent authority to link the personal and the health data of the patient. Following the creation of the code, the competent authority shall delete the personal data of the patient from the system. Paragraph 1 of Section 20 regulates that health data can only be used for statistical purposes in a way that does not allow for the identification of patients.

Paragraph 3 of Section 12 of the Privacy Act: An organization or person conducting scientific research shall be allowed to disseminate personal data only if the data subject has given his consent.

Any person carrying out scientific work may access health data of the data subject which is an implication deriving from Section 21 of the Medical Data Act.

In EESZT, according to Section 35/L of the tMedical Data Act, the operator of the Service Space shall link the patients' personal and health data with a code, replacing any information that could lead to the identification of the patient. In the Register of Self-determination the data subject/patient may limit or consent to specific data processing activities related to his/her health data in an administrative procedure, pursuant to Section 35/H. of the Medical Data Act.

What are the rights of the data subject when it comes to further processing?

Rights of the data subject connected to the original data processing activities regulated in Sections 14-15 (access to the information held about him/her, ask for information from the controller, rectification, erasure, blocking of his/her data), are applicable and the preliminary information (Section 20) to be provided to the data subject has to include the information regarding the rights and the activities. The right to object is regulated in Section 21.

What about the data subject's rights and further processing for scientific research purposes?

Since the Medical Data Act does not contain any specific regulation in this regard, the provisions of the background legislation prevail, namely the ones of the Privacy Act, the rights of the data subjects regulated under Chapter 13. According to point b) of paragraph 1 of Section 21 of the Privacy Act, data subjects may object to the processing of their personal data for the purposes of scientific research.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Pursuant to paragraph 2 of Section 21 of the Medical Data Act, the persons who inspected the data stored, the purpose and date of the inspection have to be logged. This registry has to be retained for 10 years. Certainly, this registry may be accessed by the data subjects and he/she may be informed this way, as well.

4. IV. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes

a. The impact of the GDPR on the rules applying to processing for research in the field of health

Please provide a summary of the main relevant characteristics of the new law/Bill (as far as it is relevant for processing health data for research purposes). How is (or will be) Article 9(2)(j) implemented in your country?

The first draft for the amendment of the Privacy Act, not yet submitted to the Parliament, deleted former provisions concerning processing for the purposes of scientific research. The terms of special data, biometric data, genetic data and health data are defined in the draft, and rules are laid down regarding the processing of special categories of data. According to the accompanying explanation of the legislator to the draft, sector specific legislation will contain and detail relevant requirements regarding processing personal data for purposes of scientific research, for instance. This means that Article 9(2)(j) does not seem to be implemented directly in the text of the Privacy Act. The drafts for amendment of other sector specific legislation is not available for the public.

b. Modification to the processing authorisation procedure applying to research in the field of health

No such concept as authorization procedure seems to be implied from the known text of the draft for amendment of the Privacy Act The Authority may conduct an authorization procedure on the demand of the controller or processor in the following cases: Articles 40. and 41. of the GDPR concerning codes of conduct, Article 46 (3) (a) and (b) concerning transferring data to third countries or international organisations, Article 47. concerning binding corporate rules. In respect of data protection impact assessment, the draft concerns only the preliminary consultation in case the result of the assessment indicates the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk..[19]

[19] Articles 36 (1) of the GDPR

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

How will the processing authorisation procedure (if any exists) be affected by the implementation of the GDPR? Can you describe any such change?

As presented above, there will not be an authorization procedure for the Authority in other regards than mentioned above. At this stage of the amendment no other valid conclusions or suggestions may be drawn.

What about the right of the data subject and the obligations of the controller?

Rights and obligations are proposed to be regulated pursuant to the GDPR, however these provisions do not specifically mention the processing for the purposes of scientific research, implying that the requirements are applicable for research as well.

5. Further processing for research purposes under the GDPR

The notion of further processing under the GDPR:

Recital (50) of the GDPR explains what it means by further processing. "The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.

Precisely, according to Article 5(1)(b) of the GDPR "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

How to measure the compatibility of purpose of the further processing:

Recital 50 of the GDPR further explains its considerations regarding compatibility of purpose of the further processing. "The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations. Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy."

Article 6(4) provides for the compatibility of purpose of the further processing: "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing."

The particularities of scientific research: a presumption of purpose compatibility

Recital 156 explains expectations in relation to processing for the purpose of scientific research.

"The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials."

Article 13(3) sets down requirements of providing information in relation to that processing: "Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Article 89 sets down provisions on the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes:

"Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

Given the regime applied to further processing in the GDPR, can you describe the consequences, if any, in your national legal framework?

No valid opinions may be proposed here since the final version of the national legislation, including both the Privacy Act and the vast number of sector specific legislation is not foreseen yet. The considerations made above regarding the concept of further processing and safeguards, for instance anonymizing, may be applicable here, as well.

6. Health data sources for research purposes

a. Sources of data and their regulation

Does your national framework contain specific provisions for anonymised or pseudonymised health data?

There are no specific provisions in this respect, although the anonymization is implied when the personal data is made unidentifiable, often practical approaches are the subject of considerations. The Privacy Act contains rules more in relation to personal data that may be linked to an identified or identifiable person.

In a particular provision, according to paragraph 2 of Section 12 of the Privacy Act regarding processing for the purposes of scientific research personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can attributed to an

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

identified or identifiable natural person shall be stored separately. Such data may be linked to other data if it is necessary for the purposes of research.

Paragraph 2 of Section 18 of the Medical Data Act provides that while carrying out the professional evaluations, the head of the competent organisation must make sure that the health and personal data of the patient is accompanied with a code. The code will disable the competent authority to link the personal and the health data of the patient. Following the creation of the code, the competent authority shall delete the personal data of the patient from the system. Paragraph 1 of Section 20 regulates that health data can only be used for statistical purposes in a way that does not allow for the identification of patients.

What are the different sources of health data that can be used for research purposes?

- **DIRECT COLLECTION FROM PATIENTS:**

Under the current legal framework: please explain the currently applying rules that a researcher, who intends to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.), should follow.

When health data is collected directly from a patient, he/she is entitled to be informed, and exercise data subjects' rights, including the right to object to the processing, at the same time the requirements of section 12 of the Privacy Act, and Section 21 of the Medical Data Act have to be complied with. In case of biomedical research involving human subjects, further specifications are necessary.

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.

Decree 35/2005 (VIII. 26.) of the Minister of Health on the clinical trial and application of correct clinical practices of investigational medicinal products intended for use in humans ensures the procedural guarantees of the aforementioned researches, in compliance with the provisions of the Privacy Act and the Medical Data Act, it ensures that the examination cannot be commenced without the prior written and informed consent of the individual, it ensures both the protection of individuals and their personal data, it provides for the rights of the data subjects and details the procedure of the official authorization of the research.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Yes, there is a change foreseen in the draft amendment of the Privacy Act, Section 12 disappears from there, and rules on processing on special data prevail, besides sector specific legislation might include specific rules, however the amended texts of the latter ones are not public yet.

- **COLLECTION FROM HEALTH PROFESSIONALS AND HEALTH INSTITUTIONS**

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under the current legal framework: please explain the rules currently applying that a researcher, who intends to obtain health data from medical staff, hospitals, etc., should follow.

Mainly Section 21 of the Medical Data Act is applicable, and the data subject may intervene parallelly in the registry of self-determination of the EESZT and object to any further processing activities like scientific research.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

No information is available yet in this regard.

- **PRIVATE DATABASES**

Under the current legal framework: please explain the rules currently applying for the setting up of and the use of a private database with health data for research purposes.

According to paragraph 1 of Section 21 of the Medical Data Act for the purposes of scientific research the data may be inspected with the permission of the head or the data protection officer of the health institution. The access to a private database is not prohibited by law, it depends on the permission of the head of the institution or the data protection officer, although it is required that within the scope of the relevant provisions of the Medical Data Act, the institutional and practical safeguards based on the data protection legislation are established and exercised, and that data subjects' rights are let to be practiced.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Yes, there is a change foreseen in the draft amendment of the Privacy Act, Section 12 disappears from there, and rules on processing on special data prevail, besides sector specific legislation might include specific rules, however the amended texts of the latter ones are not public yet.

- **PUBLIC DATABASES**

Under the current legal framework: do public authorities make available health data for research purposes in your country and under what conditions?

The Hungarian legislation does not differentiate between private or public database when it comes to scientific research. The legal authorization for the processing and requirements laid down in the relevant legislation is applicable in both types of institutions.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Yes, there is a change foreseen in the draft amendment of the Privacy Act, Section 12 disappears from there, and rules on processing on special data prevail, besides sector specific legislation might include specific rules, however the amended texts of the latter ones are not public yet.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

b. Application of the national framework to the AEGLE cases

Concerns of the Data Protection Authorities regarding the making use of Big Data were drawn up in a common resolution as follows:

- • To respect the principle of purpose specification.
- To limit the amount of data collected and stored to the level that is necessary for the intended lawful purpose.
- To obtain, where appropriate, a valid consent from the data subjects in connection with use of personal data for analysis and profiling purposes. •
- To be transparent about which data is collected, how the data is processed, for which purposes it will be used and whether or not the data will be distributed to third parties.
- To give individuals appropriate access to the data collected about them and also access to information and decisions made about them. Individuals should also be informed of the sources of the various personal data and, where appropriate, be entitled to correct their information, and to be given effective tools to control their information.
- To give individuals access, where appropriate, to information about the key inputs and the decision-making criteria (algorithms) that have been used as a basis for development of the profile. Such information should be presented in a clear and understandable format.
- To carry out a privacy impact assessment, especially where the big data analytics involves novel or unexpected uses of personal data.
- To develop and use Big Data technologies according to the principles of Privacy by Design.
- To consider where anonymous data will improve privacy protection. Anonymization may help in mitigating the privacy risks associated with big data analysis, but only if the anonymization is engineered and managed appropriately. The optimal solution for anonymizing the data should be decided on a case-by-case basis, possibly using a combination of techniques.
- To exercise great care, and act in compliance with applicable data protection legislation, when sharing or publishing pseudonymised, or otherwise indirectly identifiable, data sets. If the data contains sufficient detail that is, may be linked to other data sets or, contains personal data, access should be limited and carefully controlled.
- To demonstrate that decisions around the use of Big Data are fair, transparent and accountable. In connection with the use of data for profiling purposes, both profiles and the underlying algorithms require continuous assessment. This necessitates regular reviews to verify if the results from the profiling are

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

responsible, fair and ethical and compatible with and proportionate to the purpose for which the profiles are being used. Injustice for individuals due to fully automated false positive or false negative results should be avoided and a manual assessment of outcomes with significant effects to individuals should always be available.[20]

Since Big Data processing is a key point of this study, and profiling and automated decision making might be involved, the opinion of Article 29 Working Party on Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679[21] is of importance.

Regarding the Hungarian legislation Section 11 of the Privacy Act regulates the requirements in relation to decision adopted by means of automated data-process systems: "A decision which is based solely on automated process of data intended to evaluate certain personal characteristics relating to the data subject shall be permitted only if: a) it is taken in the course of the entering into or performance of a contract, provided that the request for entering into or performance of the contract was lodged by the data subject, or b) authorized by a law which also lays down measures to safeguard the data subject's legitimate interests. (2) In connection with decisions adopted by means of automated data-process systems, the data subject shall, at his request, be informed of the method that is used and its essence, and shall be given the opportunity to express his opinion."

1. Type 2 diabetes

The AEGLE project uses, after pseudonymisation, health data collected from patients who have expressed their consent with their data being used further for research purposes.

Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should the patient be informed about the new research project? Is a new patient consent, specifically focusing on the precise research project, required?

The researcher acting as data controller may carry out the research on health data with the preliminary permission of the head or the data protection officer of the health institution, based on the approved research plan. The plan of research oriented 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.

20 https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2014/10/resolution_on_bigdataaufenglisch.1.pdf.download.pdf/resolution_on_bigdata.pdf

21 http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The plan of research oriented data use 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 case the personal data are collected directly from the patients, the previous informed consent of the data subject is required in a written form.

In respect of approval by an ethical committee there is not requirement laid down in the legislation if the research concerns personal data. The anonymization of personal data for the purposes of the research is a precondition. The respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. In the course of scientific research, no copy can be made on stored data which contains personal identifying information.

In respect of clinical trials the legislation established more specific rules. The National Institute for Pharmaceuticals has published guidelines regarding the submission procedures of the research plan and the trials. The guidelines cover two fields: non-commercial clinical trials[22] and the procedure of clinical trials[23]. The guidelines contain the detailed process of the submission and approval.

In respect of Decree 23/2002. (V. 9.) of the Ministry of Health on biomedical research involving human subjects[24] 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.

The research plan is approved by the Medical Research Council. The research plan shall be approved for implementation by the executive of the healthcare institution, or in the case of another health service provider, by the executive of the regionally responsible Budapest or county inpatient institution, after receipt of the opinion of an independent professional and ethics committee made up of specialists in medicine, law, theology, ethics, and psychology, as defined in the Minister of Health Decree, in keeping with said opinion. If the committee rejects the proposal, the executive of the healthcare institution may submit a request to the MRC to revisit the opinion.

Personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can be attributed to an identified or identifiable natural person shall be stored separately.

- Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

[22] https://www.ogyei.gov.hu/non_commercial_clinical_trials/

[23] https://www.ogyei.gov.hu/clinical_trial_submission_procedure/

[24] https://net.jogtar.hu/jogszabaly?docid=a0200023.eum

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Since the more relevant rules are contained in sector specific legislation and the possible amendment of these rules is not available or known yet, no valid opinion may be provided here.

2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient's consent (after pseudonymisation).

- Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other type of approval required? From which body? Should the patient be informed about the new research project?

The same rules are applicable in respect of preparing for the research. The researcher acting as data controller may carry out the research on health data with the preliminary permission of the head or the data protection officer of the health institution, based on the approved research plan. The plan of research oriented 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 of research oriented data use 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 respect of approval by an ethical committee there is not requirement laid down in the legislation if the research concerns personal data. The anonymization of personal data for the purposes of the research is a precondition. The respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. If personal data are disseminated in the research papers, it can only be done with the previous written consent of the data subject. In the course of scientific research, no copy can be made on stored data which contains personal identifying information.

Personal data may only be inspected in the health records with the preliminary permission of the head or the data protection officer of the health care institution. The inspection functions as data transfer in terms of the Privacy Act, thus the relevant rules are applicable.

In respect of clinical trials the legislation established more specific rules. The National Institute for Pharmaceuticals has published guidelines regarding the submission procedures of the research plan and the trials. The guidelines cover two fields: non commercial clinical trials[25] and the procedure of clinical trials[26]. The guidelines contain the detailed process of the submission and approval.

[25] https://www.ogyei.gov.hu/non_commercial_clinical_trials/

[26] https://www.ogyei.gov.hu/clinical_trial_submission_procedure/

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

In respect of Decree 23/2002. (V. 9.) of the Ministry of Health on biomedical research involving human subjects[27] 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.

The research plan is approved by the Medical Research Council. The research plan shall be approved for implementation by the executive of the healthcare institution, or in the case of another health service provider, by the executive of the regionally responsible Budapest or county inpatient institution, after receipt of the opinion of an independent professional and ethics committee made up of specialists in medicine, law, theology, ethics, and psychology, as defined in the Minister of Health Decree, in keeping with said opinion. If the committee rejects the proposal, the executive of the healthcare institution may submit a request to the MRC to revisit the opinion.

Personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can be attributed to an identified or identifiable natural person shall be stored separately.

In relation to the EESZT the statement of the data subject in the records of self-determination limiting the access and use of his/her personal data has to be respected.

The data controller and the data processor may process health data only by keeping professional secrets.

- Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Since the more relevant rules are contained in sector specific legislation and the possible amendment of these rules is not available or known yet, no valid opinion may be provided here.

3. Chronic Lymphocytic Leukaemia (CLL)

The AEGLE project re-uses, after pseudonymisation, data coming from biobanks. In this instance, patients have given their informed consent for the samples and for the processing of their data. But this consent was given in general terms and not specifically for AEGLE.

- Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should the patient be informed about the new research project?

The same rules are applicable in respect of preparing for the research. The researcher acting as data controller may carry out the research on health data with the preliminary permission of the head or the data protection officer of

[27] https://net.jogtar.hu/jogszabaly?docid=a0200023.eum

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the health institution, based on the approved research plan. The plan of research oriented 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 of research oriented data use 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 respect of approval by an ethical committee there is not requirement laid down in the legislation if the research concerns personal data. The anonymization of personal data for the purposes of the research is a precondition. The respective scientific publication may not contain such health data or other personal data from which the identity of the patient could be inferred from. If personal data are disseminated in the research papers, it can only be done with the previous written consent of the data subject. In the course of scientific research, no copy can be made on stored data which contains personal identifying information.

Act XXI of 2008 on the protection of data on human genetics, on the rules of research and examinations of human genetics and of the functioning of bio-banks[28] (hereinafter referred to as Act on Human genetics) regulates specific issues related to data processing in the realm of biobanks, which is the topic concerned in the last part of this study.

The purposes of processing genetic data are specified in Section 4 of the Act of Human genetics: genetic data may be processed for the purpose of human genetic examinations and human genetic research. When personal data are processed for the purpose of research of human genetics, the data may be processed by the institute conducting the research and other people participating in conducting the research. Genetic data may be disclosed to people denoted in an authentic document and close relatives of the data subject. According to Section 6 of the Act on Human genetics the data subject is entitled to get information about his/her data generated in course of the examination of human genetics. The data subject has to receive thorough information previously to the examination, and in case of the research information has to be provided about the substance of the research and how the data subject may request to view or access the results of the research. If the genetic sample provided by the data subject will be used for research purposes, previously to signing of the consenting statement by the data subject, he/she has to receive information according to paragraph 3 of Section 159 of the Act on Health, the method of storing the genetic data and the sample, the possibilities of identification, in case of the absence of the consent of the data subject the inclusion of the genetic data in archives, and possible data transfers.

According to Section 8 of the Act on Human genetics, the preliminary informed and written consent of the data subject is necessary before commencing taking the sample. The consent must contain the consent of the data subject to that a genetic sample will be taken from him/her for the specified purpose, the sample and the relating information will be placed in a biobank and it will be transferred to another biobank, the genetic sample and the genetic data deriving therefrom will be placed in an archived collection. This statement of the data subject extends to the consent in regards of the genetic sample and data to be used for the initial purpose of the sampling, or to the use of any other purpose specified in the Act on Human genetics, or to the use of exclusively for the purpose of research.

The genetic samples and data may be used for research of human genetics according to the regulations of the Act on Human genetics. In case of research of human genetics Sections 157-164 of the Act on Health are applicable as well.

[28] https://net.jogtar.hu/jogszabaly?docid=A0800021.TV

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

There is a separate chapter in the Act on Human genetics regulating the activity of biobanks. Pursuant to Section 21 the processing and storing genetic samples and related personal data placed in biobanks has to rely on the consenting statement of the data subject under Section 8. A biobank may be maintained for conducting examinations and medical researches of human genetics by the health care service provider based on the authorization of the relevant administrative health care organ. Genetic samples and data have to be stored encrypted. The code of the pseudonymised sample or data has to be provided to the person who gave the sample for his/her exclusive use

The above mentioned rules regarding clinical trials are applicable in respect of data processing related to biobanks as well.

- Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Since the more relevant rules are contained in sector specific legislation and the possible amendment of these rules is not available or known yet, no valid opinion may be provided here.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU