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

Research Protocol by Michal Matouš and Zdeněk Kučera, at Kinstellar, s.r.o., advokátní kancelář (www.kinstellar.com)

in Prague, Czech Republic, April 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

First, we would like to get an overview of the current and upcoming legal framework applying to the processing of health data for research purposes in your country.

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.

Act No. 101/2000 Coll., on Protection of Personal Data (Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů) (the "Data Protection Act")

The Data Protection Act governs the collection and processing of personal data. It was adopted in 2000 and transposes Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[1] The Data Protection Act will be repealed by a new Act, which will implement the GDPR in the Czech Republic.

Act No. 372/2011 Coll., on the Provision of Healthcare Services (Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování) (the "Health Services Act")

The Health Services Act regulates mainly the status and role of patients and healthcare providers, the authorisation to provide health services and other relevant questions concerning the provision of healthcare in the Czech Republic. The Health Services Act also contains specific provisions relevant to data processing, in particular provisions concerning the administration of the healthcare records of patients and provisions establishing the National Health Information System.

The regulation concerning medical records in the Health Services Act establishes the obligation of a healthcare provider to keep and store medical records and use them only in compliance with the Health Services Act. It further specifies the extent of patient-related information included in such records, possible ways of administration as well as a list of persons authorised to access these medical records and to make copies. More detailed requirements concerning medical records are provided in Decree No. 98/2012 Coll. Medical records include, in addition to other necessary information, the free and informed consent of a patient as a condition for the provision of particular

[1] 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

health services, as is required under the Health Services Act as well as under the Pharmaceuticals Act (as defined below) for clinical trials.

The Health Services Act also sets up the National Health Information System, which is an integrated national information system containing and further processing data on the health status of the population, mainly for the purpose of obtaining information on the scope and quality of health services provided in the Czech Republic and for the needs of research in the field of medicine. The System further maintains the National Health Registers established to process data in various areas of healthcare. Under the Health Services Act, certain patient-related personal data may be transmitted to the System without the consent of the data subject for its further processing in the Registers.

Act No. 378/2007 Coll., on Pharmaceuticals (Zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů) (the "Pharmaceuticals Act")

The Pharmaceuticals Act mainly regulates the development, production, distribution and use of pharmaceuticals, related rights and the obligations of relevant parties. However, it also includes some provisions on data processing in relation to the regulation of clinical trials. In particular, it stipulates that clinical trials may only be performed if, *inter alia*, the rights to privacy and to the protection of personal data under special legislation are ensured for the relevant data subject.

Act No. 89/2012 Coll., Civil Code (Zákon č. 89/2012 Sb., občanský zákoník) (the "Civil Code")

The Civil Code includes certain general provisions concerning medical records and related data processing (in particular Sections 2647 to 2650). These include the obligation of a healthcare provider to maintain medical records which must clearly show information concerning the patient's health condition and on the provider's activities. The provider must keep the records as long as required for the professional care of the patient. If the records also contain information about a third person, they may not be made available without the third person's consent. Unless otherwise provided by a applicable laws (in particular the Health Services Act), the records may not be made available to any other person without the patient's express consent. The provider may only disclose information about the patient without the patient's consent in an anonymous form for scientific purposes or statistical studies concerning the health condition of the population under specific conditions stipulated in Section 2650.

As the Health Services Act includes a specific complex regulation with respect to maintenance of health records by healthcare providers (and disclosure of data to third parties) and is *lex specialis* to the provisions of the Civil Code, the applicability of the above provisions to healthcare providers is limited.

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?

The Act on Processing of Personal Data will be adopted in the Czech Republic (the "**New Data Protection Act**") and will repeal the Data Protection Act, effective as of the day of this Memorandum (1 May 2018), and implement the GDPR in the Czech Republic. In March 2018, the draft of the New Data Protection Act was approved by 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

government of the Czech Republic and presented to the Parliament. Currently, it is under discussions in the Parliament.[2] The final text of the New Data Protection Act may therefore differ from the currently available draft.

Once adopted, the New Data Protection Act will repeal the Data Protection Act in its entirety. Given that the GDPR is directly applicable, it only deals with the provisions that may be governed by the Member States. For example, under the current wording of the draft New Data Protection Act, the age for the digital consent of children with processing of their personal data is lowered to 15 years of age. However, since the New Data Protection has not been signed into law yet, it is possible that the final wording will differ from the version that is currently available.[3]

Moreover, the draft of the New Data Protection Act also transposes into the national law EU 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 offences or the execution of criminal penalties, and on the free movement of such data.

This analysis relies on the currently available wording of the draft New Data Protection Act.[4] Therefore, we recommend updating this analysis once the New Data Protection Act has been 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?

In the Czech Republic, the data protection supervisory authority is the Office for Protection of Personal Data (in Czech: *Úřad pro ochranu osobních údajů*) (the "**Office**"). It is an independent administrative authority, which is governed by the provisions of Section 28 et seq. of the Data Protection Act. Its seat is in Prague.

The Office does not play any specific role in the processing of health data for research purposes under the current legal framework; it is the general data protection supervisory authority in the Czech Republic.

The role of the Office includes[5] (i) supervision of fulfilment of obligations with respect to data processing, (ii) maintaining a register of data processing,[6] and (iii) accepting and dealing with petitions relating to data processing

[2] Due to the length of the legislative process, the New Data Protection Act will likely not be adopted before the GDPR becomes applicable in the Czech Republic, i.e. 25 May 2018.

[3] During the discussions in the Parliament, there have already been proposals to amend the draft New Data Protection Act. These proposals relate to, *inter alia*, a further lowering of the age for digital consent of children with processing of their personal data to 13 years of age, as well as lifting penalties for public authorities or public corporations (e.g. public schools or municipalities) for non-compliance with the GDPR.

[4] The New Data Protection Act is available online on the website of the Czech Parliament, see http://www.psp.cz/sqw/historie.sqw?o=8&t=138 (as of 1 May 2018).

[5] The full scope of the competency of the Office is stipulated in the Section 29 of the Data Protection Act.

[6] Currently, every data controller must notify its intention to process personal data to the Office on a prescribed online form (few exceptions from this notification obligation apply). The notification must include additional information about the intended data processing, e.g. purpose, scope of personal data, categories of data subjects, information on disclosure of personal data to third parties or transfers to third countries. This

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

(e.g. complaints from data subjects) and (iv) dealing with administrative offences and imposes fines in the event of a breach of obligations.

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

Chapter V of the draft New Data Protection Act deals with the Office, its powers and obligations and its organisation. The Office will be considered as the responsible Czech independent public authority. Such data protection authorities are governed by the provision of Chapter VI of the GDPR (Articles 51 to 59). Article 54 of the GDPR provides that each Member State must set in law the rules establishing the supervisory authority.

The role of the Office in the Czech Republic does not change significantly under the GDPR and the core principles remain the same. Under the draft New Data Protection Act, there are certain minor changes in the organisational structure of the Office (e.g. there will now be a president and two vice-Presidents of the Office) and new requirements imposed on the president (e.g. he/she must be at least 40 years of age and have certain obligatory language requirements).

The draft New Data Protection Act does not include any specific competence or powers of the Office, and Articles 55 to 59 of the GDPR apply.

The scope of tasks of the Office will change because certain obligations will no longer apply, and new ones will be imposed under the GDPR. For example, the obligation of data controllers to notify the Office about the processing of personal data prior to its commencement will no longer exist under the GDPR. Instead, the Office will receive only data breach notifications from data controllers under Article 33 of the GDPR.

The Office will publish guidelines and recommendations with the texts relating to the protection of personal data and help controllers and their processors carry out prior risk assessments. It will also encourage the drawing up of codes of conduct setting out the obligations incumbent on controllers and processors, taking into account the risk inherent in the processing of personal data for individuals' rights and freedoms.

As of the day of this analysis (1 May 2018), the Office has already started publishing on its webpage certain informal recommendations regarding the GDPR.

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 states: "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."

obligation to notify the Office prior to beginning processing will no longer apply in the Czech Republic under the GDPR/the New Data Protection 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. Transposition of Article 8.4 of Directive 95/46

In the Czech Republic, data concerning health are considered as "sensitive data" and as such may be processed only based on legal grounds stipulated in Article 9 of the Data Protection Act. Two of these legal grounds for the processing of sensitive data are the data subject's explicit consent, or if the processing is for the provision of healthcare services or the protection of public health under special laws.[7]

The old Data Protection Act does not contain any specific exception for processing health data for research purposes. Therefore, generally an explicit consent of data subjects would be required. However, as stated above, one of the exceptions for the processing of sensitive (e.g. health) data is processing related to the provision of healthcare services under the Health Services Act. Under Article 70 of the Health Services Act, the National Health Information System is set up in order to collect and process information about health conditions of the population in the Czech Republic and healthcare providers and their activities in order to obtain information about the scope and quality of healthcare in the Czech Republic, ensuring a unified provision of healthcare and adoption of a state health policy, maintenance of the National Health Registers[8] and also for the purposes of research in the field of medicine.

Under Article 70 of the Health Services Act, healthcare providers and other subjects processing personal data of patients under the provisions of the Health Services Act are obliged to provide to the Health Information System various personal data (including health data) of patients. The scope of personal data may include identification of the patient (including birth number), data about the duration of illness and its treatment, family health background, need for further medical treatment, etc.

Section 72 of the Health Services Act stipulates the purpose of the National Health Registers and enumerates subjects having access to the data they contain. Authorised persons with access are primarily healthcare professionals that provide treatment to patients.

The data from the National Health Registers might also be provided to institutions for statistical and research purposes; however, in this case all provided data must be anonymised.

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?

The Data Protection Act does not introduce any specific regime that would apply to data processing for research in the field of health purposes. It only introduces two exceptions that involve data processing for research purposes.

The first exception is stipulated in Article 5, Section 1, Letter e) of the Data Protection Act and concerns the duration of data processing. It contains an exception from the general rule that personal data may be processed for no longer

[7] E.g. the maintenance of health records under the Health Services Act.

[8] There are currently 12 different National Health Registers in the Czech Republic, such as the National Oncology Register, National Register of Hospitalised Persons, National Register of Drug User Patients, etc.

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

than is necessary for the purpose for which the personal data was collected. It stipulates that personal data may be processed after this time for research purposes. In this case, the controller must take into account the protection of personal and private life of individuals and anonymise the personal data as soon as possible.

The other exception is stipulated in Article 11, Section 3, Letter a) of the Data Protection Act and concerns the information obligation towards data subject. The provision states that in the event (i) the data controller has not obtained personal data from the data subject, (ii) the data controller processes personal data solely for scientific purposes, and (iii) provision of information to the data subject would involve a disproportionate effort or disproportionate costs, then the data controller is not obliged to provide the data subjects with information regarding the processing of his/her personal data.

Despite the two above provisions, the Data Protection Act does not introduce a specific regime, and the data controller must always meet all obligations with respect to such data processing.

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

Under the Data Protection Act the researchers (as data controllers) might be exempted from obligations to (i) process personal data only for as long as is necessary for the purposes for which the personal data was collected or (ii) provide data subjects with information regarding the processing of his/her personal data.

Please see the paragraph above for more information.

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?

Under the Data Protection Act, the processing of personal data for scientific research purposes is not a specific exception as foreseen by Article 8.4 of the Directive.

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?

Personal data concerning health (including any information that the healthcare provider obtained in connection with providing the healthcare services) is protected by professional secrecy of healthcare professionals, and a breach of this obligation constitutes an administrative offence.[9]

Article 51, Section 2 of the Health Services Act lists the situations under which a healthcare provider may disclose such information and which situations are not considered as a breach of the professional secrecy obligation. These include situations where:

[9] Article 51 of the Health Services 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

1. disclosure of information is necessary for subsequent treatment of the patient;
2. the patient has exempted the healthcare provider from the professional secrecy obligation;
3. information is disclosed based on provisions of the Health Services Act or another law, and such law provides that the information can be disclosed without the patient's consent (e.g. transmitting information to the National Health Information System); and
4. disclosure of information is necessary for the purposes of criminal procedure.

The professional secrecy obligation of healthcare providers applies also with respect to deceased subjects.

For minors or other persons that do not have full legal capacity, the rights regarding health data are exercised by their parents or other legal guardians. These persons have access to the health records of the patient and may grant consent to the disclosure of his/her health data. A healthcare provider may refuse to provide the information to parents or guardians of the patient if there is a suspicion that the patient is being abused and providing this information could further threaten the patient.

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

Under Article 11, Section 3, Letter a) of the Data Protection Act researchers, as data controllers, might be exempted from obligations to provide data subjects with information regarding the processing of his/her personal data.

This exemption applies in the event that (i) the data controller has not obtained personal data from the data subject, (ii) the data controller processes personal data solely for scientific purposes and (iii) providing the information to the data subject would involve a disproportionate effort or disproportionate costs, then the data controller is not obliged to provide the data subjects with information regarding the processing of his/her personal data (all conditions must be met cumulatively).

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?

The Data Protection Act does not introduce a specific regime that would apply to data processing for research in the field of health purposes and general provisions regarding penalties apply.[10] The maximum penalty for a breach of obligations under the Data Protection Act is CZK 10 million (approx. EUR 392,000). In practice, the Office has never imposed any penalty that would exceed 50 per cent of the maximum penalty.

[10] Article 45 of the Data Protection 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

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?

Under the current Czech regime, a data controller is obliged to notify the Office about the intention to process personal data.[11] The notification must include additional information about the intended data processing, e.g. purpose, scope of personal data, categories of data subjects, information on the disclosure of personal data to third parties or transfers to third countries.

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

As stated above, except for two specific provisions applicable to processing for research purposes, the Data Protection Act does not introduce a specific regime for processing health data for research purposes. Therefore, the general obligation that further processing must be compatible with the purpose of the processing for which the data was collected also applies.

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

To be lawful, further processing must be compatible with the purpose of the processing for which the data was collected. Personal data is collected for a certain purpose and may not be further processed in a manner which is incompatible with this purpose. As a general rule, personal data may be further processed for a different purpose only if the data controller has a legal basis for such further processing (e.g. if the data subject has granted his/her consent).

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

Under the Data Protection Act, there are no specific conditions for the further processing for scientific research in the field of health purposes. The general obligation with respect to compatibility with the original purpose applies.

Exemptions from the notification obligation and/or obligations to notify data subjects might apply, provided that conditions described above are met.

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

The data subject must first be informed about further processing in accordance with the provisions of the old Data Protection Act. The exception from this obligation applies if the data subject has already been provided with such

[11] Article 16 of the Data Protection 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

information or if the personal data was not collected directly from the data subject and the conditions under Article 11, Section 3 of the Data Protection Act have been met.

The data subject has general rights relating to data processing, i.e. right of access to personal data, right of rectification of personal data (e.g. blocking, correction or liquidation), right to withdraw consent (provided that the personal data is processed based on consent).

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

Please see the two exceptions above that apply to scientific research purposes.

4. 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?

Under Article 9 (2) of the GDPR national legislation may further regulate the processing of sensitive data in a variety of areas, including health, archiving and other important public interests. The draft New Data Protection Act, however, does not further regulate this area and does not utilise the possibility provided under Article 9(2)(j) of the GDPR.

Furthermore, the related Article 89 of the GDPR allows for other exceptions and derogations in processing for scientific research. However, the draft New Data Protection Act does not introduce any new regulation and does not utilise the possibility provided under Article 89 of the GDPR.

Although the draft New Data Protection Act does not explicitly address the processing of health data for research purposes, Sections 16 to 21 of the draft New Data Protection Act regulate the processing of personal data for journalistic purposes or for the purposes of academic, artistic or literary expression.

According to the explanatory notes to the draft New Data Protection Act (which further clarify the meaning and purpose of its particular provisions), the above-mentioned provisions may also be applied to scientific research activities, including processing of health data for scientific purposes, provided that such processing is proportionate to the legitimate interests of the data subjects.

Section 17 of the draft New Data Protection Act introduces exceptions from the general information obligations of a data controller if fulfilment of those obligations in practice would be detrimental to the purposes of the scientific research. In such case, appropriately informing the data subject about the identity of the controller is sufficient if the data subject may obtain detailed information, for example, on the website of the controller.

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

Nevertheless, it is unclear whether (and to what extent) these Sections 16 to 21 of the draft New Data Protection Act will indeed apply to scientific research and we recommend to await further guidelines in this respect. Also, as explained above, the New Data Protection Act is still being discussed in the Parliament, and its wording as of 1 May 2O18 can further be changed.

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

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

As previously mentioned, the general obligation to notify the Office of all data processing[12] will no longer exist once the GDPR becomes directly applicable in the Czech Republic. The draft New Data Protection Act Does not introduce any new authorisation procedure in this respect.

However, conducting research in the field of health may involve, inter alia, processing of health data on a large scale. Since health data constitute a special category of data within the meaning of Article 9(1) of the GDPR, it is likely that researchers (as data controllers) might be obliged to carry out a data protection impact assessment under Article 35 of the GDPR.

Once the data controller has carried out a data protection impact assessment, and the results of the assessment indicate that the processing would result in high risk in the absence of measures to be taken by the controller to mitigate such risks, then the controller will need to consult the Office in accordance with Article 36 of the GDPR. If the Office is of the opinion that the intended processing would be in breach of the GDPR, the Office will have to provide advice to the controller and/or may use its powers under Article 58 of the GDPR. The draft New Data Protection Act does not utilise the possibility provided under Article 36 (5) of the GDPR and does not introduce any other obligatory consultations with or authorisations from the Office in relation to processing for the performance of a task carried out in the public interest, including processing in relation to social protection and public health.

In the event that the controller already processes personal data as part of its legal obligations prior to the GDPR becoming applicable, it is not obliged to conduct a data protection impact assessment.

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

Under Article 89 (2) of the GDPR, the national law can provide for derogations from the rights of data subjects under the GDPR if the personal data are processed, inter alia, for scientific research purposes. However, this derogation is only possible if providing the data subjects with their rights would likely render impossible or seriously impair the achievement of the scientific research purpose.

The New Data Protection Act does not introduce any specific derogations from the rights of data subjects and obligations of the controller for the purposes of research in the field of health. Therefore, the controller generally has information obligations towards the data subject under Articles 13 and 14 of the GDPR (as applicable).

[12] Section 16 of the Data Protection 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

Section 11 of the draft New Data Protection Act provides for some limited general derogations from the rights of data subjects and obligations of the controller, under which information obligations towards data subjects do not have to be fully observed. These derogations are based on the legal ground provided for under Article 23 (1) of the GDPR and relate to, inter alia, important objectives of public interest in matters of public health. In the event that the controller intends to act on these derogations (i.e. not fulfil its information obligations towards data subjects), it must notify the Office of the limitation without undue delay and state the circumstances under Article 23 (2) of the GDPR. Applicability of the provision of Section 11 of the draft New Data Protection Act for the purposes of research in the field of health is questionable and will likely be limited only to specific circumstances where there is a risk of serious harm in the area of public health (i.e. in case of emergency).

5. Further processing for research purposes under the GDPR

The notion of further processing under the GDPR:

Further processing can be defined as "the processing of personal data for purposes other than those for which the personal data has been initially collected". Further processing is allowed only when its purpose is compatible with the purpose for which the data has been initially collected. Further processing for a compatible purpose of personal data is possible using the same legal basis as the one used for the initial processing. For example, if personal data is initially processed based on the data subject's consent, then further processing for a compatible purpose is possible on the same legal basis. In other words, it isn't required to contact the data subject again for a new consent authorising the further processing of the same data.

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

Further processing for a purpose other than that for which the personal data has been collected is governed by Article 6 (4) of the GDPR. In particular this article tries to address how to measure whether or not the purpose of the further processing is "compatible". This is particularly relevant to big data analytics. Article 6 (4) establishes a test to measure such compatibility.

Where this processing is not based on the data subject's consent, or EU or Member State law, but on another legal ground, the controller will ascertain the compatibility of the processing's purpose with the initial purpose stated during the data collection. To do so the controller will take several elements into account, in particular: any link between the initial purpose and the further processing purpose, the context of the collection and the relation between the data subject and the controller, the nature of the data, in particular if it is considered to be sensitive data under Article 9 of the GDPR. The controller will also consider the possible consequence of further processing for the data subject and the existence of appropriate safeguards. If the result of the test is positive for the controller and shows that none of the elements have been significantly altered to make the further processing unfair or illicit, no further legal basis is necessary for the further processing. If this is not the case, then the further processing will have to rely on a separate legal basis.

If this test is successfully met, then the further processing is possible. However, it will be up to the data controller to demonstrate the compatibility of the purposes.

The particularities of scientific research: a presumption of purpose compatibility

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

Processing of personal data for the purposes of scientific research is an exception from the above rule. Under Article 5 (1) (b) of the GDPR compatibility of the processing purpose of further processing with the initial purpose of the collection is presumed under Article 89 (1). Here the GDPR establishes a presumption of compatibility of purposes for scientific research purposes. The reasoning behind this exception can be easily imagined. Scientific research is very often based on existing data; this is why allowing the processing of personal for different (if not incompatible) purposes is fundamental for scientific research.

This assumption made for the benefit of scientific research is linked to the derogation of the principle of data minimisation for scientific research purposes. However, this presumption is limited by some requirements, which are set out in Article 89(1) of the GDPR: the appropriate safeguards for the data subject's rights and freedoms, and ensured technical and organisational measures, such as pseudonymisation. Although a different scenario would require different technical and organisational measures to ensure the safeguards for the data subject's rights and freedoms. This is clearly indicated in Recital 156 of the GDPR: "The further processing of personal data for (…) scientific (…) research purposes (…) is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which does not permit or no longer permits the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data)."

Additionally, further processing of personal data is connected to the principle of storage limitation (Article 5(1)(e) of the GDPR), as it also constitutes a derogation from that principle, "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject".[13]

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

In its Section 6 the draft New Data Protection Act introduces two additional exemptions, under which the data controller is not obliged to assess the compatibility between the original purposes of processing and purposes of further processing, which would otherwise be required under Articles 6(1) and 5(1)(b) of the GDPR. These two exceptions cover situations where the data controller processes personal data for additional purposes insofar as the data controller processes personal data in order to safeguard protected interests, and this further processing is necessary and required for (i) fulfilment of a statutory obligation of the data controller or (ii) fulfilment of a task carried out in the public interest, which is stipulated by legal regulation, or while performing public authority.

The "protected interests" include, inter alia, important matters of public health. These two exemptions are based on Recital 50, Article 6 (4) and Article 23 of the GDPR. The possibility of further processing, without assessing the compatibility of the original and additional purposes that would otherwise be required under Articles 6 (4) and 5 (1) (b) of the GDPR is thereby extended to other cases, in addition to processing for scientific or research purposes as stipulated under Article 5 (1) (b) of the GDPR.

[13] Adopted from the French report.

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

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?

In the current legal framework, the Data Protection Act defines anonymised data in its Section 4 (c) as data that either in its original form or after processing cannot be related to a specified or identifiable data subject. Anonymised data are not considered as personal data, and as such are not subject to regulation under the Data Protection Act.

Moreover, according to Section 5 (e) of the Data Protection Act, the controller is obliged to store personal data only for the period necessary for the purpose of processing. After this time, personal data may be retained for scientific purposes, but they should be anonymised as soon as possible.

In the revised legal framework, the New Data Protection Act does not include any specific provisions for anonymised or pseudonymised health data.

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.

Health data, or data concerning health status and genetic data of the data subject, are considered as sensitive data under Section 4 (b) of the Data Protection Act. Under Section 9 of the Data Protection Act, sensitive data can only be processed if the data subject provided explicit consent to the processing. Before the data subject grants consent, the data subject must be provided with various information about the processing, including the purpose of the processing, the scope of the personal data concerned, the controller involved in the processing and the time period for which the consent applies. The controller is obliged to inform the data subject in advance of her/his rights of access to personal data, the right to rectify personal data, and other rights set forth in Section 21 of the Data Protection Act. The researcher, as a data controller, must be able to demonstrate the data subject's consent with the processing of his/her personal data throughout the entire processing.

Under Section 16 of the Data Protection Act, any person who intends to process personal data as a data controller is obliged to notify the Office of this processing in writing. The notification must include the following information: identification of the controller, the purpose of the processing, the categories of data subjects and their personal data concerned, personal data sources, a description of the personal data processing, the place(s) where the personal data will be processed, the recipients or categories of recipient, the expected transfer of personal data to other countries and a description of the safeguards for ensuring the protection of personal data.

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

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

After the GDPR comes into effect, the provisions of the Data Protection Act will no longer apply. The draft New Data Protection Act does not contain any special provisions in relation to research/scientific purposes and the obligations that the researchers will have to follow will be governed by the GDPR. Specifically, processing of special categories of personal data are regulated by Article 9 of the GDPR.

As previously mentioned, the obligatory notification to the Office will no longer be required prior to commencing the personal data processing. However, the researcher, as a data controller, will likely be obliged to conduct a data protection impact assessment[14] and designate a data protection officer under Articles 35 and 37 of the GDPR.

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

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.

Maintenance of the medical records of patients by healthcare professionals and health institutions is governed by Sections 53 to 64 of the Health Services Act. The Health Services Act sets out an obligation of a healthcare provider to keep and store medical records and to use them only in compliance with the obligations set out by the Data Protection Act and other relevant statutory provisions. These medical files also contain patients' personal data, including sensitive data.

Processing patient health data and other related data is also governed by Sections 2647 to 2650 of the Civil Code. The Civil Code imposes an obligation on healthcare providers to maintain medical records, and this must include information about the patient's health conditions and on the provider's activities.[15] These records may not be made available to any other person without the patient's express consent.[16] The healthcare provider may only disclose such information without the patient's consent in an anonymous form and for the purposes of scientific research concerning the health condition of the population.

The Health Services Act further establishes the National Health Information System which collects data obtained from healthcare providers and health institutions for the needs of research in the field of medicine. Personal data concerning patients may be transmitted to the National Health Information System without the data subject's consent. These data can then be made available to researchers at their request, however, only in form that does not allow and identification of the patients.

In addition to the obligations already specified, healthcare facilities are obliged to comply with the relevant conditions for the processing of personal data provided for in the old Data Protection Act, including the obligation according to which personal data can be processed only in accordance with the purpose for which it was collected, unless a special law stipulates otherwise.

Section 5 (6) of the old Data Protection Act also addresses the possibility of the controller processing personal data to transmit it to another controller only under the required conditions. These include the data of the data subject to

[14] Including a prior consultation with the Office, where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

[15] Section 2647 of the Civil Code

[16] Section 2649 of the Civil Code

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

be either obtained in connection with the activity of the controller or already disclosed publicly and that the data subject has been informed in advance of this procedure and has not opposed it.

Moreover, transmission of the data by health professionals must be always done in a manner guaranteeing confidentiality of the data. Under Section 15 of the old Data Protection Act the processional secrecy requirements extend also to the controller's personnel.

As already mentioned above, under Section 16 of the Data Protection Act a notification to the Office is required before commencing the processing.

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

After the GDPR comes into effect, the provisions under the old Data Protection Act will no longer apply and the draft New Data Protection Act does not address the conditions of access to data gathered by health professionals and healthcare establishments. The rules researchers will have to follow will be governed by the GDPR, as well as special provisions set out in the Health Services Act. The change for researchers as controllers is that no mandatory notification will be required prior to the commencement of personal data processing.

- **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.

While the processing of health data is in principle prohibited, it is possible to do so if the data subject has given his/her explicit consent as stated above. When creating a private database containing health data, such database must be notified to the Office, following the procedure set out above. Moreover, in case the database is to be hosted by a third party (as data processor), the hosting of health data must be the subject of a contract between the host and the data controller.[17]

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

The draft New Data Protection Act does not specifically address the rules applying to the set up and use of a private database with health data, so the GDPR provisions shall apply.

- **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 Ministry of Healthcare is the founder of the National Health Information System regulated by the Health Services Act. It serves as an unified national information system established primarily to process data provided by health professionals and health institutions on the health status of the population, in order to obtain information on the scope and quality of health services provided and for the need of science and research in the field of health.

[17] Section 6 of the 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

According to Section 70 (2) of the Health Services Act, certain personal data concerning patients are transmitted to the National Health Information System by healthcare provider without the consent of the data subject. These concern (i) the data necessary for identification and place of residence of the patient, (ii) data related to his or her health status in relation to disease and its treatment, in particular socio-demographic and diagnostic data, personal, family and occupational history of the patient related to the disease, including an assessment of the patient's current state of health, data on the health services provided to the patient, as well as data on the patient's profession or employment, or the performance of the service necessary for assessing the patient's state of health, (iii) the identity of the healthcare provider and (iv) the identification data of the last employer (for patients with an occupational disease).

Currently, the data concerning health are further processed in 12 National Health Registers established and maintained by the National Health Information System. The relevant scope of information transmitted by health service providers to the National Health Registers is further specified in the data standard of the Ministry of Healthcare and the binding methodological guidelines for the National Health Information System.

The records in the registers do not include the names, surnames and addresses of patients as data subjects or any detailed personal characteristics.

Individual data from the registers is not publicly available. Data from the registers is provided only in aggregate form (e.g. for territorial units, for types of health facilities, for diagnosis groups, for individual diagnoses). Non-aggregated anonymised personal data can be provided from the database only for scientific and research purposes. Except for cases where register data are directly used in the provision of healthcare, it is not important to identify the person connected to the data, but whether the reported cases in the registers belong to the same person or to different persons.

Data protection in these health records is high. Access to individual data is only granted to subjects specifically authorised by the administrator of the database and to health service providers. The majority of authorised workers are healthcare workers who enter data into the appropriate register and see only "their input data". The number of other authorised staff who have access to all data of a particular register is strictly limited.

When processing personal data in registers, all the requirements set out by the Data Protection Act must be complied with. After a fixed deadline, individual data gathered in the registers is anonymised by an unidirectional encryption algorithm.

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

Under the revised legal framework, the rules applicable to the use of public databases do not substantially change.

b. Application of the national framework to the AEGLE cases

In the AEGLE project, the "research objective is to establish the use of Big data analysis in the prediction of outcomes in three working scenarios: Chronic Lymphotic Leukemia (CLL), Intensive Care Units and type 2 diabetes for 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

prediction of adverse outcomes. The research methodology is Big Data analysis to establish predictive values that may apply in three clinical scenarios and to see if this can be generalised to other healthcare disease models". [18]

To achieve its objective, the AEGLE project must base its approach on the study, and thus the processing, of data concerning health. This section aims to address each of the three proposed AEGLE cases, and to determine the requirements in general terms for access and the processes relevant to data under the Directive (the current framework) and the GDPR.

1. Type 2 diabetes

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

Current legal framework:

Under Czech legislation there are no special provisions that would directly concern the data processing for research in the field of health; therefore, general provisions of the Data Protection Act will apply.

As individual data from the registers is not publicly available, the researcher at first has to be granted access to the database by filling a request for access to the Health Registry System.

Moreover, as a person who intends to process personal data, the researcher is obliged to notify its intention to the Office in writing before beginning to process any personal data. The notification will have to include all the required information as stated above.[19]

In this case, when personal data has not been obtained from the data subject, the information and instruction described above under Section 11 might not have to be provided by the controller, because the personal data will be processed solely for scientific purposes, and the provision of such information would likely require disproportionate efforts or unreasonably high costs. However, the controller is required to take necessary measures against unauthorised intrusion into the private and personal life of the data subject.

Once the GDPR has been implemented:

The draft of the New Data Protection Act does not address the processing of personal data for research in the field of healthcare and it leaves the general regulation to the GDPR.

Under the GDPR, notification to the Office prior to the processing of personal data is no longer mandatory. However, the controller must carry out a data protection impact assessment of the envisaged processing operations when there is a high risk of rights violation presumed for the data subject.[20] If the assessment indicates a need to further address risks, prior to processing, the controller must consult the Office.[21]

[18] AEGLE Grant Agreement, Annex 1, p. 83.

[19] Section 16 of the Data Protection Act

[20] Article 35 GDPR

[21] Article 36 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

The GDPR also sets the obligation for the controller and processor to designate a data protection officer in specified cases, including these when core activities of controller consist of processing on a large scale of special categories of data, including data concerning health.[22]

To demonstrate compliance with the GDPR, a controller may obtain a Personal Data Protection Certificate or commit to comply with the Code of Conduct, both of these still only on a voluntary basis.[23] For now this possible guideline created at the sectoral level is not available in the Czech Republic. The draft New Data Protection Act further addresses only the entity responsible for accreditation of the entities entitled to issue the Certificate. In the Czech Republic this entity is the Czech Accreditation Institute, o.p.s.

The data subject must be informed in conformity with the provisions set out in the GDPR. Further processing is allowed only when its purpose is compatible with the purpose for which the data has been initially collected. In the case presented above, there is no legal requirement to contact the data subjects again for a new consent authorising the further processing of the same data.

2. Intensive Care Unit (ICU)

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

The data is collected by health professionals in ICU services when they are treating patients. The processing of this data for research in the field of health assumes a compatible purpose.

Current legal framework:

Under the provisions of Section 9 of the Data Protection Act concerning sensitive data and according to the respective obligations set out in the Civil Code and in the Health Services Act,[24] unless otherwise provided by an applicable legal regulation, patients' health records may not be made available to any other person without the express consent of the patient. The healthcare provider may disclose information about the patient without the patient's consent for purposes of scientific research only if these are provided in an anonymous form.[25]

It is possible for health professionals to transfer the data they have collected to research; however, the recipient will be obliged to adhere to professional secrecy. Additionally, the data subjects will have to be informed about the transfer, and they may oppose it.

Otherwise, a similar procedure of notification to the Office and information obligations as described in the first scenario shall apply.

Once the GDPR has been implemented:

[22] Article 37 GDPR

[23] Articles 40 and 42 of the GDPR

[24] Sections 2647-2650 of the Civil Code and Sections 53-69 of the Health Services 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

Since the data was collected by healthcare provider in ICU services for the purposes of providing healthcare to the patient (e.g. within the scope of the provision of healthcare under the Health Services Act), it may be provided to AEGLE only with express consent of the patient and information on data processing in compliance with the GDPR.

Alternatively, it might be provided to AEGLE as anonymous data.

Otherwise, general principles for the data processing under GDPR as mentioned in the first scenario shall apply.

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:

In this case, we understand that the data were collected by biobanks for research purposes and consent with processing of sensitive personal data as required under Section 9 of the Data Protection Act was granted by data subjects. Even though the purpose AEGLE seeks to achieve is considered compatible with the initial purpose (i.e. research in the field of health), under current legal framework is not clear whether such consent would be in fact considered as sufficient for research carried out by AEGLE. As a result, we would recommend obtaining an express consent from data subjects specifically granted to AEGLE for such reuse of data obtained from biobanks.

Otherwise, a similar procedure of notification to the Office and information obligations, as described in the first scenario, shall apply.

Once the GDPR has been implemented:

Similarly as under current legal framework, we understand that the data were collected by biobanks for research purposes and consent with processing of sensitive personal data as required under Article 9 of the GDPR was granted by data subjects. Even though the purpose AEGLE seeks to achieve is considered compatible with the initial purpose (i.e. research in the field of health), it is not clear whether such consent would be in fact considered as sufficient for research carried out by AEGLE under legal framework after the GDPR becomes applicable. As a result, we would recommend obtaining an express consent from data subjects specifically granted to AEGLE for such reuse of data obtained from biobanks.

We note that the Office might further clarify the recommended approach in the future and we recommend updating this memorandum in the event such clarification from the Office is available.

Otherwise, general principles for data processing under the GDPR as mentioned in the first scenario shall apply.

Personal data sets may be subject to additional conditions of use by the data source; moreover, health data is protected by professional secrecy, and this obligation also applies to recipients of this 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