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

Research Protocol by Boris Dvoršćak, attorney at law,

in Zagreb, 30 March 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 Tecnologies 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. The legislative and regulatory instruments regulating the processing of health data for research purposes (current regime)

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 Personal Data Protection Act (Official gazette number 103/2003, 118/2006, 41/2008 and 130/2011, in Croatian as *Zakon o zaštiti osobnih podataka*, hereinafter as the "**Act**")

The Act is the main Croatian regulation governing the collection and processing of personal data, including special categories of personal data and (further) processing for scientific purposes. The Act was first adopted in 2003 and has been amended in 2006, 2008 and 2011 for the purpose to transpose the 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 (hereinafter as the "**Directive**").

The Act prescribes misdemeanour fines for breaches of its provisions on the collection and processing of personal data, in the range of HRK 20,000 – 40,000 (around EUR 2,650 – 5,300). However, as the Croatian Data Protection Agency still does not have the right to directly impose fines (it can merely initiate a misdemeanour procedure before competent court) such fines are very rarely imposed in practice.

The Act will cease to be effective on 25 May 2018, when it will be replaced by the entirely new act which will be enacted for the purposes of implementation of the GDPR. The unofficial translation of the Act may be found on the following link:

http://www.legislationline.org/documents/id/19201

The Healthcare Act (Official gazette 150/2008, 155/2009, 71/2010, 139/2010, 22/2011, 84/2011, 154/2011, 12/2012, 35/2012, 70/2012, 144/2012, 82/2013, 159/2013, 22/2014, 154/2014, 70/2016, 131/2017, in Croatian as *Zakon o zdravstvenoj zaštiti*)

The Healthcare Act regulates the provision of healthcare services, the organization of healthcare services in Croatia and the supervision of such services. The act also provides provisions on the protection of professional secrecy in relation to health professionals.

The Act on the Protection of Patient's Rights (Official gazette 169/2004, 37/2008, in Croatian as *Zakon o zaštiti prava pacijenata*)

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The act regulates and determines the rights of patients while using health related services and the protection of such rights. The act contains very limited privacy related provisions and states that patients are entitled to the privacy of data related to their health status in accordance with the regulations on the protection of professional secrets and the provisions of the Act. Also, patients are entitled to determine persons that may be informed on their health status.

The act prescribes a monetary misdemeanour fine for breaching the patients' privacy rights in the amount of HRK 10,000 -50,000 (around EUR 1,300 – 6,660) in relation to health institutions and HRK 5,000 – 10,000 (around EUR 650 – 1,330) in relation to employees of health institutions.

The Croatian Criminal Act (Official gazette 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, in Croatian as *Kazneni zakon*)

The Croatian Criminal Act determines most criminal acts, conditions for criminal responsibility and associated penalties.

In relation to personal data, the act defines unauthorized use of personal data as a separate criminal act. Collection, processing or usage of personal data contrary to the provisions of the Act and/or other acts regulating specific data processing is punishable by up to one year imprisonment. More severe cases of the criminal act (e.g. if the perpetrator acquires significant monetary gains as a result of the act, in case the criminal act is committed in relation to minors or in relation to sensitive data) are punishable by up to three years imprisonment. If the perpetrator of the criminal act in question is an official person, the prescribed penalty ranges from six months up to five years of prison.

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

Do shared electronic patient records exist in your country? How is the sharing of electronic patient records regulated? Can data stored in these records be used for research purposes?

Electronic patient records exist in Croatia and they are maintained by the patients' general physician and are then sent to the Central Health Information System of the Republic of Croatia (in Croatia as *Centralni informacijski sustav zdravstva Republike Hrvatske*, hereinafter as "**CEZIH**"). The data delivered to CEZIH may be used by the Croatian Health Insurance Fund, Ministry of Health, Institute of Public Health for the purposes of drafting mandatory annual reports and for statistical purposes.

All medical data processed by general physicians and CEZIH in relation to electronic patients' records is protected by professional secrecy rules and the provisions of the Act.

The Ordinance of the Usage and Protection of Data from Medical Documentation of Patients Maintained by CEZIH (Official gazette 14/2010, in Croatian as *Pravilnik o uporabi i zaštiti podataka iz medicinske dokumentacije pacijenata u Centralnom informacijskom sustavu zdravstva Republike Hrvatske*) allows authorized users of electronic patient records (i.e. physicians) to share specific health data of patients with other providers of medical services, exclusively for the purpose of providing medical services to the patient.

As the usage of data stored in these records is defined by the aforementioned ordinance, such data may not be used for research purposes. However, under the provisions of the Act, such data may be transferred to researchers for

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

medical research purposes, provided that adequate protection measures are applied in the sense that such data is anonymized and that the identification of patients is no longer possible in any manner.

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.

What are the main characteristics of the legislative implementation of the GDPR in your country?

What is your own assessment of the legislative approach adopted in your country for implementing the GDPR?

The draft of the new GDPR compliant act under the name the Act on the Implementation of the General Data Protection Regulation (in Croatian as *Zakon o provedbi opće uredbe o zaštiti podataka*, hereinafter as "**Act Proposal**") was published for public consultations on 21 February 2018.

Under Croatian law, the public consultations procedure lasts for 30 days, after which the proposed amendments are accepted or rejected by the competent authority (in this case Ministry of Administration), and the Act Proposal should be sent to parliament for its enactment. Provided that the public consultations will not result with major changes of the Act Proposal, it may be expected that the Act Proposal will be implemented by the end of April 2018.

The Act Proposal will fully replace the Act and its adjacent bylaws. It is expected that the bylaws will be amended on an ad hoc basis.

As the GDPR is directly applicable, the Act Proposal, apart from provisions defining the new role of the Croatian regulator (as described below), deals with the following provisions of the GDPR which allow Member States to adopt a modified approach:

Processing of Genetic Data

Any processing of genetic data for the purposes calculations of chances of illness and other serious health issues as part of execution of life insurance policies is forbidden, unless data subjects provide their explicit consent. This provision applies to all data subjects entering into life insurance agreements in Croatia, if the data controller is seated or provides its services in Croatia.

Processing of Biometric Data

The Act Proposal imposes further restrictions for processing of biometric 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Public authorities and private entities may process biometric data only if such processing is defined by law and is necessary for the protection of individuals, assets, classified information or professional secrets, provided that the interests of data subjects that contravene such processing do not prevail. Processing of biometric data necessary for fulfilment of international treaties related to identification of data subjects during crossing of state borders shall be considered as lawful.

Private entities may process biometric data for the purposes of safe identification of users of services, only based on an explicit consent given by the users in accordance with the provisions of the GDPR.

Processing of biometric data (e.g. fingerprints, eye-scans) for the purposes of working time recording or entry/exit of working premises is allowed only on the basis of a legal obligation or if the employer has provided an alternative mechanism for such purposes (e.g. signature list) and the data subjects provided an explicit consent in accordance with the provisions of the GDPR.

Processing of Personal Data through Video Surveillance

Although GDPR, as a technology neutral regulation, provides no special rules related to video surveillance, the Act Proposal imposes special rules on such processing.

Data controllers (or processors) must provide a clear notification to data subjects that a premises (or part of it) is under video surveillance. Such notification must be visible while entering the perimeter of surveillance at the latest, and contain the information provided in Article 13 of the GDPR. Also, a clear and understandable photograph (sticker) must be attached to the notification containing i. information that the object is under video surveillance; ii. information on the data controller; and iii. contact details of the data controller for possible complaints.

In relation to work premises, such premises may be put under video surveillance by the employer only if the conditions under the work safety regulations have been met, and all employees have been notified in advance on the existence of video surveillance. Premises intended for rest, hygiene and changing room may not be put under video surveillance.

In relation to residential buildings, video surveillance may be installed in such building under the condition that 2/3 of all owners agreed. However, only access to the building's entrance and exit and common premises (e.g. stairways) may be put under video surveillance. Video surveillance used for the purposes to control the effectiveness of cleaners and other staff working in residential building is forbidden.

Administrative Fines

Administrative fines may not be imposed to public authorities and bodies (and responsible individuals employed with such bodies).

Responsible persons in data subjects (e.g. directors, management board members) may be imposed with an administrative fine for infringements of the GDPR. The administrative fines range between HRK 5,000 – 500,000 (around EUR 660 – 66,000).

In addition, the Act Proposal imposes a special administrative fine in the amount of up to HRK 50,000 (around EUR 6,660) for breaching of the provisions related to video surveillance, which is in direct conflict with the provisions of the GDPR on administrative fines and their amounts.

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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?

Under the Act, the Croatian Data Protection Agency (in Croatian as *Agencija za zaštitu osobnih podataka,* hereinafter as "**CDPA**") is an independent authority, reporting only to the Croatian Parliament via its annual reports.

The main public functions of the CDPA are:

- supervision of personal data protection;
- maintaining of the registry of databases of personal data;
- supervision of transfers of personal data outside of Croatia;
- issuing opinions on personal data protection matters and the application of the Act;
- providing suggestions and opinions for the further development of personal data protection;
- initiating criminal and misdemeanour procedures before competent public authorities.

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

The Act Proposal modifies the functions and authority of the CDPA in accordance with the GDRP. The CDPA is still organized as an agency, entirely independent from the Croatian Government and other public institutions, and is only responsible to the Croatian Parliament.

The most important changes relate to the CDPA's supervisory authority as it will now be able to conduct previously announced inspections, as well as "dawn raids". Also, the CDPA now obtained the authority to directly impose administrative fines for breaches of the GDPR (as opposed to the Act, under which it could only initiate misdemeanour procedures). An appeal against the imposition of administrative fines is not possible, but the fined entity may initiate an administrative procedure before the locally competent administrative court.

Also, the CDPA is now obliged to issue its professional opinions on private data protection issues, within a period of 30 days following the request of any private individual or entity.

2. Transposition of Article 8.4 of Directive 95/46

Article 8 of Directive 95/46 prohibits, in principle, the processing of special categories of personal data concerning health. Article 8.2 lists a series of exceptions to this general prohibition. Article 8.4 states "Subject to the provision of suitable safeguards, Member States

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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".

When transposing Directive 95/46 did your national legislator or supervisory authority make use of the power granted to Member States in Article 8.4 of the Directive? Did the legislator use this provision to insert any additional (i.e. additional to the exceptions listed in the Directive) exemption (to the prohibition to process health data) for the processing of health data for research purposes?

If yes, how is such an exemption formulated? Please explain.

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?

How is such an exception formulated, and does it set out specific conditions?

Under the Act, data concerning health is considered as a special category of personal data and as such its processing is prohibited save for specially listed activities, as set out in Article 8.2 of the Act:

- if the data subject gave consent to such processing;
- if the data processing is necessary for the purposes of carrying out rights and obligations of the data controller defined by special regulations;
- if the processing is carried out within the scope of legal activity of an institution, association or any other non-profit entity with political, religious or other aim, provided that such processing relates solely to the members of this entity, and that the data obtained is not disclosed to a third party without prior consent of the data subject;
- if data processing is necessary to establish, obtain or protect claims prescribed by law;
- if the data subject personally published such data; or
- if data processing is necessary for the purpose of preventive medicine, medical diagnosis, health care or management of health institutions, on the condition that the data is processed by a health official based on rules and regulations adopted by competent authorities.

These activities completely encompass the activities set out in Article 8.2 of the Directive.

The Croatian regulator did not make use of the power granted to Member States in Article 8.4 of the Directive by setting our additional exemptions.

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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?

What is the scope?

Which are the steps, and who are the key actors?

Under Croatian law, there is no specific regime applying to data processing for research in the field of health purposes, although certain provision of the Act and the Act on the Protection of Patients' Rights apply.

Article 6.2 of the Act prescribes that personal data may be further processed only for the purposes that are compatible to the purposes in which such data was initially processed. However, further processing of personal data in historical, statistical and scientific purposes will not be deemed as incompatible, provided that appropriate technical measures are conducted. The Act is silent on the kind and extent of such measures, however the data must be supplied to the recipient in the manner that the identification of data subjects is no longer possible (unless the data subject gave his explicit consent which covers such processing).

Also, until 25 May 2018, there is an obligation imposed to all data controllers to notify the CDPA and register each established data processing activity and personal data databases with the public registry maintained by the CDPA. In practice, the CDPA already does not expect data controllers to conform to this obligation and unofficially advises data controllers to register personal data databases only if explicitly ordered by the CDPA to do so.

The Healthcare Act prescribes that the provisions on the protection of professional secrets apply, apart from health professionals, also to all other persons which, as part of their activities, gained access to health data of patients, which includes also researchers.

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

For what reasons?

From which provisions?

What are the consequences?

In Croatia researchers are not exempt from the generally applicable data protection provisions.

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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?

In Croatia there is no exemption as foreseen by Article 8.4 of the Directive.

However, certain safeguards apply in relation to the processing of patient's health and other personal data outside medical treatment procedures as already explained above under points II. A. and II. B., which relate to the identification of the patient whose health and other personal data are processed for scientific-research purposes (e.g. conducing of technical measures which provide identification of the data subject, i.e. patient, impossible).

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?

Health and other personal data of patients must be handled in accordance with the professional secrecy principles and the provisions of the Act. Article 126 of the Healthcare Act prescribes that all healthcare professionals as well as other employees of health institutions are bound by professional secrecy in relation to any information on the health state of a patient. The same obligation applies to all other persons who, while conducting their activities, gain access to health information of patients.

Under the Act and other regulations, there are no provisions related to express consent for specific data (apart from the general provision that sensitive data may be processed on the basis of the data subjects' consent).

The Act is silent in relation to data processing of deceased data subjects. However, the CDPA issued a formal opinion, under which the provisions of the Act do not encompass deceased data subject, as they cannot be considered as private individuals, as defined by the Act. Therefore, personal data of deceased data subjects may be freely collected and processed, under the condition that such processing does not directly concern personal data of certain other data subjects.

There are no specific provisions for minors or persons subject to guardianship in relation to the processing of their health data for the purposes of studies and research and therefore all of the above mentioned rules apply.

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

Article 9 of the Act provides that before any personal data is collected, the data controller or data processor must inform the data subject on:

- the identity of the data controller;
- the purpose of the processing of personal data;
- on the data subjet's right of access and correction of personal 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- on the data recipients or categories of data recipients;
- whether the collection of personal data is compulsory or voluntary and the possible consequences in case of data subject's refusal to provide data (in case the collection of personal data is obligatory, the legal basis for collection must also be stated).

The above information is provided to the data subject regardless of whether the personal data is collected from the data subject directly or indirectly.

Article 9.4 of the Act provides that the above information does not have to be provided to the data subject if the data is, for statistical, historical or scientific research purposes transferred to recipients or collected from already existing databases of personal data or would incur a disproportionate effort or the processing of personal data is explicitly provided by law.

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?

There are no specific penalties if the conditions for processing of personal data for scientific research in the field of health purposes are not respected.

However, Article 36 the Act prescribes a general penalty in the amount of HRK 20,000 – 40,000 (around EUR 2,650 – 5,300) for data controllers that transfer personal data to recipients for the purposes of scientific research in a way that the data subjects are identifiable. The fine in the same amount is prescribed if the data controller did not inform the data subject in accordance with Article 9 of the Act (as described above).

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

This section is relevant if the regime applying to processing for research in the field of health is a specific regime. But it may not always apply, and in such an instance the processing is ruled by the general regime.

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?

Where in the applicable legislation can it be found?

What are this regime's main steps and conditions?

In Croatia, any processing of personal data (including sensitive data) is governed by the general regime for processing of personal data under 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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

Article 6.2 of the Act prescribes that personal data may only be collected and processed for a purpose of which the data subject is informed of, which is specific and lawful. Further processing is allowed only if the purpose of such further processing is compatible with the purpose of the primary collection and processing of personal data.

However, further processing for statistical, historical or scientific research purposes is deemed compatible to the purposes of the primary collection and processing of personal data, provided that appropriate technical measures were conducted. The Act is silent on the kind and volume of such technical measures and there is no case law provided by the CDPA.

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

Please see the above answer.

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

In Croatia, there are no specific conditions to the further processing for scientific research in the field of health purposes. The general rules of the Act apply to such further processing, as described in the previous answers above.

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

In Croatia, the data subject's rights in relation to further processing of personal data are the same as the general rights of data subjects under the Act.

As described above in more detail, Article 9 of the Act prescribes that data subjects have the right to be informed of, among others, the purposes for collection and processing of personal data, data recipients or categories of data recipients, data subject's rights of access and correction of personal data etc.

Furthermore, Article 19 of the Act prescribes that the data controller is obliged, in a period no longer than 30 days following such request of the data subject, to:

- deliver a confirmation whether personal data relating to the data subject is processed;
- provide information in an understandable form on the data subject's data that is processed and the sources from which such data was obtained;
- allow access into the database of personal data related to the data subject, which databases must contain the purpose and legal basis of the collection, processing and usage of such data;
- deliver information on the person to which the data subject's data were given for usage, the purpose and legal basis of such transfer;
- provide information on the logic of any automated processing related to the data subject's personal 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under Article 20 of the Act, the data controller has an obligation to, on the basis of the data subject's request, to amend, complement or erase personal data if such data is incorrect, incomplete or outdated or if their processing is not conducted in accordance with the Act.

Irrespective of the data subject's request, the data controller is obliged to amend or delete personal data on his own initiative, if he establishes that that personal data that is processed is incomplete, inaccurate or outdated.

The data subject must be informed on any amendment/erasure described above in a period of 30 days following such amendment/erasure.

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

There are no specific data subject's rights related to further processing for scientific research purposes, apart from the general rights of data subjects as described in the previous answer.

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

Under the GDPR the processing of health data for research purposes is regulated by Article 9(2)(j), which authorises the processing of health data if this *"processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject" (emphasis added), and is combined with Article 89(1) ("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").*

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

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 Act Proposal does not further regulate the processing of health data for research purposes in any manner, nor does it implement Article 9 (2) (j). Therefore, the provisions of the GDPR shall be applied directly.

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?

Is it a logical change?

Is the supervisory authority involved? If yes, how?

In Croatia, processing authorization procedure does not exist and is not envisaged by the Act Proposal. Therefore, the GDPR has no effect to the researches in the field of health in this regard.

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

Article 89 (2) of the GDPR provides the opportunity for Member States to derogate from: the right to access the data by the data subject, the right to rectify, the right to restrict the processing and the right to object. However, these derogations are only available if those rights would seriously impair or make impossible the scientific purpose of the processing.

As the Act Proposal does not contain any such derogations it appears that the government did not intend to build upon the opportunity to provide derogations to some rights of data subjects.

5. Further processing for research purposes under the GDPR

Further processing of personal data for scientific research purposes is regulated in the GDPR by Article 5(1)(b) ("further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1),

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

not be considered to be incompatible with the initial purposes") and Article 89(1) ("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?

As the GDPR will be directly applicable, the provisions of Article 5 (1) (b) and Article 89 (1) will directly apply in Croatia as well. As Article 6.2 of the Act already provides that further processing for statistical, historical or scientific research purposes is deemed compatible to the purposes of the primary collection and processing of personal data, provided that appropriate security measures were conducted, the GDPR will not change the current legal framework in that regard.

However, as the Act is silent on the kind and scope of such measures and there is no available case law published by the CDPA, the GDPR in Article 89 (1) broadens the regime in the regard that it defines pseudonymisation as an example of such measure, as well as further processing which does not permit the identification of data subjects.

6. Health data sources for research purposes

This section seeks to identify information on the availability of health data for research purposes. Do public authorities or other entities facilitate the availability of health data for research purposes? In what way? Under what conditions?

Croatian public authorities and other entities do not facilitate the availability of health data for research purposes in any specific manner.

The collection and processing of health data outside medical treatment of patients is permitted only if such collection and processing is based on the patients consent, or other persons who have the right to consent on behalf of the patient in case the person is not capable of giving consent by himself. This does not apply to deceased patients and their data may be freely collected and processed, as the Act does not apply to deceased persons.

If consent of patients is not obtained, health data may be further processed for historical, statistical or scientific research purposes, under the condition that such data is supplied to the data recipient in an anonymized form without the possibility to determine the identity of the patients, as stipulated in Article 11.4 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

a. Sources of data and their regulation

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 is sensitive data and so in principle its processing is prohibited. However, as already explained above in answer II.A., the Act provides exceptions to such prohibitions, under which sensitive data may be processed.

Therefore, a researcher who intends to collect health data directly from individuals for research purposes, needs to obtain a consent for such collection and processing. In addition, the individual would need to be informed on such processing pursuant to Article 9 of the Act, as explained in more detail in answer II.C. above.

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

As the Act does not in any manner regulate the processing of sensitive data, the provisions of Article 9 of the GDPR will be directly applicable in Croatia.

Apart from consent as a legal basis, researchers will be enabled to make use of Article 9 (j) of the GDPR which allows processing of sensitive data if such processing is necessary for statistical, historical or scientific research purposes, provided that such processing is conducted in accordance with Article 89 (1) of the GDPR, and appropriate safety measures are provided.

In addition, patients would need to be informed on the collection and processing of their health data, in accordance with Articles 13 and 14 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.

Collection of health data from health professionals and health institutions is possible under certain conditions.

The Acts permits the collection and processing of health data outside medical treatment of patients only if such collection and processing is based on the patients consent, or other persons who have the right to consent on behalf of the patient in case the person is not capable of giving consent by himself.

Therefore, the patients would need to provide their consent to the health professionals and health institutions which are providing them medical treatment, in which they would need to consent to the transfer of their medical data to

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

researchers for medical purposes. This does not apply to deceased patients and their data may be freely collected and processed, as the Act does not apply to deceased persons.

If consent of patients is not obtained, the Act prescribes that health data may be further processed for historical, statistical or scientific research purposes, under the condition that such data is supplied to the data recipient (researchers in this case) in an anonymized form and without the possibility to determine the identity of the patients.

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

Please see answer above on collection of health data directly from patients.

- **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 creating a private database containing health data is not prohibited, its legal basis must be carefully applied. Indeed, 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. Until 25 May 2018 such a database must also be notified to the CDPA within a period of 15 days following the establishment of such database, according to Article 16 of the Act.

However, if the database is used for scientific research purposes, then the rules already explained above apply (i.e. rules regarding further processing for research purposes etc.).

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

Please see answer above on collection of health data directly from patients.

- **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 Ordinance of the Usage and Protection of Data from Medical Documentation of Patients Maintained by CEZIH (Official gazette 14/2010, in Croatian as *Pravilnik o uporabi i zaštiti podataka iz medicinske dokumentacije pacijenata u Centralnom informacijskom sustavu zdravstva Republike Hrvatske*) provides that health data in the public database maintained by CEZIH may be used only for the purposes of providing healthcare services. In addition, the stated ordinance prescribes that health professionals and institutions may share specific health data of patients with other providers of medical services, exclusively for the purpose of providing medical services to the patient.

As the purpose for which health data in the public database may be processed is explicitly defined by the aforementioned ordinance, such data may not be used for research purposes.

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under the revised legal framework the rules applicable to the use of public databases described above do not effectively change.

b. Application of the national framework to the AEGLE cases

This section seeks a short summary of the rules to be observed in your country by a hypothetical researcher involved in the AEGLE project. The objective is to obtain a practical response for informing such a researcher as clearly as possible.

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:

The operations realised in the AEGLE project qualify as processing for research purposes in the field of health, and therefore the provisions of the Act regarding sensitive data apply.

If the health data is collected directly from patients, consent must be obtained for the collection and processing of such data. If the data has been collected indirectly from healthcare professionals during their activities, then they may transfer the data to researchers in a way that the patient's identity is anonymised and cannot be identified.

Researchers will also be bound by professional secrecy for this data. Also, the patients would need to be properly informed on the processing of their health data by researchers in accordance with Article 9 of the Act and as explained in more detail in answer II.C. above (with the explained exceptions on collection of personal data from already existing databases).

Revised legal framework:

As already explained above, the Act does not in any manner regulate the processing of sensitive data nor further processing for scientific research purposes and therefore provisions of Article 5 (1) (b) and Article 9 of the GDPR will be directly applicable in Croatia.

Apart from consent as a legal basis, researchers will be enabled to make use of Article 9 (j) of the GDPR which allows processing of sensitive data if such processing is necessary for statistical, historical or scientific research purposes, provided that such processing is conducted in accordance with Article 89 (1) of the GDPR, and appropriate safety measures are provided.

In addition, patients would need to be informed on the collection and processing of their health data, in accordance with Articles 13 and 14 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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

2. Intensive Care Unit (ICU)

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

Current legal framework

The operation realised in the AEGLE project qualifies as processing for research in the field of health purposes, therefore the already explained rules regarding the processing of personal data (including sensitive data) for research purposes apply.

As pseudonymised data is still considered under the Act as personal data and the Act is silent on the technical measures that need to be conducted in relation to further processing for scientific research (unofficially, we were informed from the CDPA that such measures are strictly interpreted), consent from patients for such collection of health data should be obtained.

In case consent from patients is not obtained as explained above, the respective health data should be sent to researches as recipients of data in an anonymised form, without the possibility to identify the data subjects in question.

Revised legal framework

Please see answer under VI.B.1.

3. Chronic Lymphocytic Leukemia (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:

The operation realised in the AEGLE project qualifies as processing for research in the field of health purposes, therefore the already explained rules regarding the processing of personal data (including sensitive data) for research purposes apply.

As pseudonymised data is still considered under the Act as personal data and the Act is silent on the technical measures that need to be conducted in relation to further processing for scientific research (unofficially, we were informed from the CDPA that such measures are strictly interpreted), consent from patients for such collection of health data should be obtained specifically for the purposes of AEGLE.

Otherwise, the respective health data should be sent to researches as recipients of data in an anonymised form, without the possibility to identify the data subjects in question.

Revised legal framework

Please see answer under VI.B.1.

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 Tecnologies Limited, UPPSALA UNIVERSITET, UNISR, Time.Lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU