'Big data analytics' and processing of health data for scientific research purposes : the Polish legal framework

Research Protocol by Dariusz Adamski
in Wrocław, Poland *, 29 March 2018, updated 05 June 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 of 29 August 1997 on the Protection of Personal Data (Pol. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997, Nr 133, poz. 883, with further ammendments); hereinafter: PDPA 1997.

This Act governs the collection and processing of personal data. While Poland was not a member of the EU when the legislation was adopted, the Bill was enacted to implement the directive 95/46 and has closely followed its standards. On 25 May 2018 it was replaced by an entirely new Act, which bears the same title as the previous Act (hereinafter: PDPA 2018).[1]

- Act of 28 April 2010 on the System of Information in Healthcare (Pol. ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, Dz. U. 2011 r., Nr 113, poz. 657, with further amendments)

This piece of legislation contains specific provisions on public healthcare databases and electronic medical documentation they process. It lists government healthcare databases brought together in what is called the System of Information in Healthcare (SIH). In practice SIH databases do not comprise one integrated system, but rather a cluster of databases and registers administered by various institutions, used for different purposes and accessed by different entities for different purposes.

The provisions of this Act of relevance for this study's topic deal in particular with electronic medical documentation. According to Art. 11 of the Act on the System of Information in Healthcare all service providers are required to maintain medical documentation in electronic form (Sec. 1), in the formats published by the minister in charge of health (Sec. 1a). Service providers are obliged to use standardised protocols for the exchange of electronic medical records (Sec. 1b). Medical data, including personal data and individual medical records, contained in the electronic

[1] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000.

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

medical documentation of the service recipient, stored in an IT system of the service provider, are made available to authorised recipients via the SIH. In principle data sharing requires a consent of the patient (Sec. 2). Medical documentation stored in the SIH should enable downloading by another healthcare provider (Sec. 3) of at least the information specifically prescribed by the Act. The information covers, among others, the identification data of the service provider, the data of the healthcare recipient, identification of the medical employee who participated in the medical event reported in the documentation, identification of the medical employee who created the documentation and inserted it into the relevant database, information on the medical event reported in the documentation, information on the issued prescriptions (Sec. 4). The majority of the above information should be introduced to the SIH system immediately, no later than one day after the end of the relevant medical event, and the rest ought to be introduced there in the real time (Sec. 5).

The Act on the System of Information in Healthcare establishes categories of the data recipients authorised to access the data contained in the SIH databases directly through the system. This group is restricted to healthcare recipients, healthcare providers and authorities in charge of health insurance and supervision (Art. 12.3-8). The same Act (Art. 12.2) provides that "access to the data processed in the SIH depends on the authorisations held by the users of the system on the basis of this Act or the provisions on personal data and unitary medical data". As this rule applies to the users of the system only, and as the Act specifically establishes who could be considered as a user of the system, the quoted provision does not establish an access regime for other data recipients. Art. 11.8 fills up this gap, providing that other recipients may access medical documentation otherwise than through the SIH system in accordance with the Act of 6 November 2008 on Patients' Rights and the Patient Rights Ombudsman, discussed below.

- Act of 6 November 2008 on Patients' Rights and the Patient Rights Ombudsman (Pol. ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Dz.U. 2009 nr 52 poz. 417, with further amendments)

One part of this Act – on medical documentation – should be summarised here. According to it, medical documentation contains at least personal data of the patient, the identification of the entity providing health services with an indication of the organizational unit at which the health services were provided; the description of the patient's state of health or healthcare services provided to him or her, as well as the date of creating the documentation (Art. 25.1). Furthermore, the entity providing health services is obliged to keep, store and provide medical documentation in the form specified in this Act and in the Act on the System of Information in Healthcare, as well as to ensure the protection of its data (Art. 24.1). The Act further establishes that medical documentation should be accessed only in order to protect health, to provide and to manage the provision of health services, to maintain the ICT system in which the medical documentation is processed, and to ensure its security and only by the persons representing the medical profession and by the personnel performing auxiliary activities in the provision of health services, as well as the activities related to the maintenance of the ICT system, based on specific authorizations of the data controller (Art. 24.2). The personnel authorised to access medical documentation is obliged to keep confidential the information related to the patient obtained in connection to the performance of its tasks. The confidentiality requirement applies also after the patient's decease (Art. 24.3). Processing of medical documentation may be outsourced to a processor, in the sense of data protection rules, if the processor maintains the same level of data protection and the controller retains the right to control the way medical documentation is processed (Art. 24.4). The processor is also obliged to keep the information confidential (Art. 24.6).

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

Medical documentation can be accessed by the patient or his/her statutory representative or a person authorized by the patient (Art. 26.1) as well as by other providers of health services, if the documentation is necessary to ensure the continuity of healthcare services, and by public authorities in charge of supervision and inspection of healthcare providers, as well as by insurers and providers of technical maintenance of the databases storing medical documentation (Art. 26.3). It can also be made available to authorised educational institutions, as long as it is necessary for educational purposes (Art. 26.3a). What is particularly relevant for this study, *medical documentation may also be made available to a university or a research institute for scientific purposes, without revealing the name and other data enabling the identification of the person to whom the documentation relates* (Art. 26.4).

Electronic medical documentation is made accessible according to the Act on the System of Information in Healthcare (Art. 26.5). Medical documentation can be made available by, among others, electronic means of communication and on a (tangible) electronic data carrier (Art. 27.1). The healthcare provider who makes electronic documentation available should keep a record of its disclosures, identifying the documentation, of the person disclosing it and of the recipient (Art. 27.4). The Act also authorises the healthcare institutions making its medical documentation available to other entities to charge a fee, as far as the documentation is made available in excerpts, physical copies, printouts, scans, or on a tangible electronic data carrier (Art. 28.1). The Act also establishes maximum fees chargeable in such situations (Art. 28.4).

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?

On 25 May 2018 the PDPA 2018 replaced the Act of 1997. The new legislation provides for detailed rules in some of the areas where the GDPR leaves a scope for national discretion. In particular, it makes some of the rights established by the GDPR inapplicable to certain controllers performing public functions. It also provides for technical rules, supplementary in comparison to the GDPR, on data protection officers, accreditation, certification and certification bodies, codes of conduct, the President of the Office for Personal Data Protection, procedures applicable when the provisions on the protection of personal data are violated, the European administrative cooperation, inspection procedures, civil liability, administrative fines and penal sanctions.

The Act does not purport to regulate other areas where the GDPR leaves the national legislator scope for enacting more specific provisions. For example, this is the case for the consent of children: the government has chosen not to lower the age of consent to under 16, which is why the PDPA 2018 contains no provision on the age of consent.

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?

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

Within its mandate, the Polish data processing authority monitors how administrators processing health data (primarily providers of healthcare services) apply data protection rules and acts accordingly when it finds breaches of the rules in force. But, when doing so, it does not approach either health data or research activities in any specific manner.

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

The status of the Polish data protection authority will not change dramatically under the new legislation. The relevant institutional provisions are established in a separate chapter (No. 6) of the PDPA 2018.

The Authority changed its name, from the previous Inspector General for Personal Data Protection into the President of the Office for Personal Data Protection (pol. *Prezes Urzędu Ochrony Danych Osobowych*, hereinafter: PUODO). According to Art. 34.1-2 of the Act, PUODO is the competent authority for the protection of personal data and a supervisory body within the meaning of Regulation 2016/679, Directive 2016/680 and Regulation 2016/79. The term of office of PUODO is four years (Art. 34.6). He or she must be a Polish citizen, have a university degree, be distinguished by legal knowledge and expertise in the field of personal data protection, enjoy full public rights, and cannot be convicted by a valid sentence for an intentional crime or an intentional fiscal offense, as well as have a good reputation (Art. 34.4). The same person cannot hold the office for more than two terms (Art. 34.7). PUODO shall be appointed and dismissed by the lower chamber of the Parliament (pol. *Sejm*) with the consent of the upper chamber (pol. *Senate*) (Art. 34.3) and can be dismissed before the end the term of office only if he or she resigns, becomes permanently unable to perform his or her duties as a result of illness confirmed by a medical certificate, offends the vow, or has been sentenced by a valid court decision for committing a deliberate crime or an intentional fiscal offense, as well as he or she has been deprived of public rights (Art. 34.9). PUODO enjoys legal immunities and further safeguards of his/her independence (Arts 38-44).

Among other potentially relevant institutional provisions it should be indicated that PUODO is to present to *Sejm*, the Council of Ministers, the Ombudsman, the Ombudsman for Children and the Prosecutor General a report on his/her activities, including, in particular, information on the number and the type of final court decisions on data protection involving PUODO's decisions and on the state of compliance with the provisions on the protection of personal data (Art. 50). He or she opines draft legislative acts regarding personal data (Art. 51) and may address state bodies, local self-government bodies, state and municipal organizational units, non-public entities performing public tasks, natural and legal persons, organizational units which are not legal entities, and other entities with motions seeking to provide effective protection of personal data (Art. 52.1). PUODO may also request the competent bodies to exercise their legislative initiative regarding the protection of personal data (Art. 52.2). Furthermore, PUODO publishes on its website standard contractual clauses referred to in Art. 28.8 Regulation 2016/679, approved codes of conduct referred to in Art. 40 Regulation 2016/679 and the standard data protection clauses governed by Art. 46.2.d Regulation 2016/679, as well as recommendations on technical and organisational measures used to maintain data processing security (Art. 53). He or she also publishes a list of types of personal data processing operations referred to in art. 35.4-5 Regulation 2016/679 (Art. 54) and can run an IT system allowing data controllers to report breaches of personal data protection referred to in Art. 33 Regulation 2016/679 (Art. 55). PUODO, by way of a decision, approves binding corporate rules referred to in Art. 47 Regulation 2016/679 and grants the permits referred to in Art. 46.3 Regulation 2016/679 (Art. 56). The Act also provides for a procedure of prior consultation

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

referred to in Art. 36 Regulation 2016/679 (Art. 57). Finally, if PUODO finds that there has been a violation of the provisions on the processing of personal data, he or she may request the perpetrator to enforce disciplinary or other legal measures against the persons responsible and to inform the office, within a specified time limit, about the results of such proceedings and the actions taken (Art. 58).

2. Transposition of Article 8.4 of Directive 95/46

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

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

a. Transposition of Article 8.4 of Directive 95/46

The scientific purposes exception is established by Art. 27.2.9 PDPA 1997. According to it, sensitive data can be processed when "it is necessary to conduct scientific research, including preparation of a dissertation required to obtain a university diploma or university degree; publishing the results of scientific research cannot take place in a way that allows for an identification of the persons whose data has been processed." Polish law has not established any more specific rules on processing sensitive personal data for research purposes.

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?

No such a regime has been established by Polish law.

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

First, if personal data is necessary for scientific, didactic, historical, statistical or public opinion research purposes and if its processing does not violate the rights or freedoms of the data subject, the controller is exempt from informational obligations (the identity and address of the data controller, the purposes of processing, data sources

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

and data subject's rights when it collects the data from other sources than the data subject) under the additional condition that fulfilling the obligations would be excessively expensive or would jeopardize the achievement of the objective of the study (At. 25.2.3 PDPA 1997). This exemption corresponds with a provision located in the section of the Act on data subject's rights. Accordingly, the controller may refrain from informing data subjects about processing of their data for scientific purposes when this would entail outlays disproportionate to the purposes (Art. 32.4)

Second, processing of personal data for a purpose other than that for which it was collected is acceptable if it does not violate the rights and freedoms of the data subject, if it is performed for the purposes of scientific, didactic, historical or statistical research and if it is based on one of the legitimate bases of processing corresponding with Art. 7 Directive 95/46 (implemented by Art. 23 PDPA 1997) as well as complies with the abovementioned rules for processing personal data obtained from other sources than the data subject (Art. 26.2).

Third, as mentioned earlier, the Act authorises processing of sensitive personal data for scientific purposes, if additional conditions are met (Art. 27.2.9).

Fourth, data controllers are exempted from the obligation to register the data filing system with the supervisory authority if they process personal data in order to prepare a dissertation required to obtain a university or academic degree (Art. 43.1.10).

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

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

The only requirement directly established by the Polish implementation of Art. 8.4 of the directive 95/46 concerns anonymisation of the data in the published outcome of the research. In the context of suitable safeguards it is also worth highlighting that, while the provision implementing Art. 8.4 of the directive waives the prohibition of processing sensitive data, the controller is nonetheless obliged to follow the remaining obligations established by PDPA 1997, including the conditions for exemptions from its certain other provisions, as indicated in Sec. II.B of this report.

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?

Pursuant to the Act on Patients' Rights and the Patient Rights Ombudsman, all the data concerning health is protected by professional secrecy. As indicated in Sec. I.A of this report, it follows from it that medical records may be processed for scientific purposes only when they are anonymised (Art. 26.4 of the Act on Patients' Rights and the Patient Rights Ombudsman). Of course, this provision applies if the data subject does not permit for a different

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 regime. If he or she does, the consent prevails over the default method or processing health data established by the Act on Patients' Rights and the Patient Rights Ombudsman.

Under the Polish system prior to the GDPR no specific provisions apply to data protection of deceased data subjects, minors, or to persons subject to guardianship.

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

Assuming that the answer to this question is limited to sensitive personal health data, it further depends on whether the information is collected from the data subject or a third person. If it is collected directly from the data subject, his or her consent will determine the terms of processing the data, while all the related informational requirements would apply to the controller. If, however, the information is obtained from another person (e.g. a medical institution), the recipient of the information should not obtain it in any other form than anonymised. As such information is not personal data any longer, the recipient would not be bound by any provisions on data protection. The same will apply under the GDPR, because the prohibition of processing of personal data in medical records by other entities than those statutorily authorised to do so stems from the law separate from PDPA 1997, which will remain in force even when the latter is revoked.

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?

While the purpose of processing may influence the severity of sanctions, it does not determine the legal qualification of the offence. In this respect the important aspect is the possible violation of the rules of processing sensitive personal data.

This latter violation faces the same penalties both according to the PDPA 1997 and the PDPA 2018.

According to Art. 49.2 PDPA 1997 whoever processes personal data in a filing system, when the processing is not legitimate and the data reveals racial or ethnic origin, political views, religious or philosophical beliefs, religious, party or trade union membership, data on health condition, genetic code, addictions or sex life, the perpetrator is subject to a fine, or imprisonment for up to 3 years.

Analogously, pursuant to Art. 107.2 PDPA 2018, whoever illegitimately processes personal data revealing racial or ethnic origin, political views, religious or ideological beliefs, trade union membership, genetic data, biometric data processed to identify a physical person, health data, sexuality or sexual orientation is subject to a fine, restriction of liberty or imprisonment for up to three years.

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?

No further formalities are required by the Polish legal system.

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

According to PDPA 1997 the exact rules to apply in this case depend on whether the data is obtained directly from the data subject or from third parties.

In the first of the cases the controller should inform the data subject of the scope and the data subject should unambiguously express his or her consent in this respect.

When the data is obtained from a third party, in principle processing of personal data for a purpose other than that for which it was collected is authorised if it does not violate the rights and freedoms of the data subject, if it is performed for scientific, didactic, historical or statistical research purposes and if it is based on one of the legitimate bases of processing personal data, as well as if it otherwise complies with the abovementioned rules on processing personal data obtained from other sources than the data subject (Art. 26.2, as indicated in Sec. II.B of this report). This authorisation does not apply to medical files, however, because a separate *lex specialis* Act on Patients' Rights and the Patient Rights Ombudsman precludes a disclosure of non-anonymised medical records.

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

According to Art. 26.1 PDPA 1997 the data controller who processes personal data should act with due care in order to protect the interests of data subjects. It is in particular obliged to ensure that personal data is processed in accordance with law, that it is collected for legitimate purposes and *not subject to further processing incompatible with these purposes*, that the data is factually correct and adequate in relation to the purposes for which its is processed; and that it is stored in a form allowing for identification of the data subject, as well as no longer than it is necessary to achieve the legitimate purpose of processing. This rule is subject to the exception indicated earlier (Art. 26.2 PDPA 1997).

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

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

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

The prohibition of further processing applies to personal data on health if the data is obtained directly from the data subject, unless – of course – the data subject has consented to such processing after obtaining appropriate information from the data controller. On the other hand, under the Act on Patients' Rights and the Patient Rights Ombudsman specific conditions for further processing of personal data for scientific purposes established by the general data protection system become irrelevant when the medical information is to be received from third parties (e.g. healthcare service providers), because this information, when comprising the broad notion of medical documentation, can be made available to research institutions only after anonymisation.

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

There are no additional rights granted to the data subject by PDPA 1997 in relation to further processing.

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

There are no specific rights granted to the data subject by PDPA 1997 in relation to further processing for 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?

The PDPA 2018 does not govern processing personal data for research purposes. As such, it does not provide for a derogation indicated in Art. 89.2 or Art. 89.3 GDPR. In consequence, controllers of such personal data should abide by all their obligations and all data subject's rights established by the Regulation, unless the data they receive is pseudonymised in line with Art. 89.1 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

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

Once the controller has made a data protection impact assessment and the results indicate high risks in the absence of measures taken to limit such risks, then the controller will consult the competent supervisory authority.[2] The Authority can take action within eight weeks. However, Article 36.5 GDPR leaves the opportunity to the Member States to further regulate this issue for processing carried out in the public interest, in particular for social protection and public health. Polish law does not take up this opportunity.

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

The implementation of the GDPR will not entail any processing authorisation procedure, as the Polish PDPA 2018 does not use the opportunity, established in Art. 36.5 GDPR, to require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing in relation to public health.

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

As indicated earlier in this section, the Polish PDPA 2018 does not provide for any derogations permitted according to Art. 89.2 and 89.3 GDPR. In consequence, controllers of such personal data should abide by all their obligations and all data subject's rights established by the Regulation.

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. It is, in other words, not required to contact the data subject again for a new consent authorising the further processing of the same data.

[2] Article 35 and 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

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 none of the elements have been significantly altered to make further processing unfair or illicit, no further legal basis is necessary for the further processing. If this is not the case, then 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

However, the processing for scientific research purpose is an exception. Indeed, under Article 5.1.b of the GDPR the 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 data 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 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 preamble 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 GDPR), as it also constitutes a derogation to that principle, because "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".

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

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

The rules set out by the GDPR will be directly and exclusively applicable. Among the provisions other than Art. 89.1 GDPR, the regime will rely in particular on the purpose limitation established by Art. 5.1.b GDPR and the additional obligations imposed on the data controller by Art. 13.3 and Art. 14.4 GDPR.

The prohibition of processing non-anonymous medical information, which is established by a separate provision in the Polish legal system, is not to be considered as conflicting with these rules. Instead, arguably it should be assumed that Polish law requires processing of anonymous medical data obtained from medical files as "the appropriate safeguard for the rights and freedoms of the data subject", in the sense of Art. 89.1 GDPR.

6. Health data sources for research purposes

a. Sources of data and their regulation

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

As mentioned earlier, further processing – also for research purposes - of medical data enclosed in medical files can only take place if the data is anonymised.

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 is sensitive data and so in principle its processing is prohibited. However, this prohibition does not apply to processing for scientific research purposes under Art. 27.2.9 PDPA 1997, if the additional requirement of refraining from publishing personal data in any publications related to the research is also obeyed. In consequence, the controller is authorised to process personal health data if it complies with all the obligations and data subject's rights otherwise established by the Act for processing of personal data obtained directly from the data subject. Processing of such personal data can also take place either on the basis of an explicit consent or another legitimate interest, in the sense of Art. 7.1.f directive 95/46.

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

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

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

This is highly unlikely, as it can be assumed that currently health data are collected for research purposes either directly from data subjects, on the basis of their explicit and informed consent (e.g. medical trials) or it is obtained from the institutions holding medical files. In the first of the two scenarios new rules will apply *mutatis mutandis*, with due consideration of the alterations in the obligations of the controller and the rights of the data subject according to the new legal regime established by 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.

The crucial rule applicable in this scenario is that external researchers cannot obtain access to medical documentation in any other form than anonymous. Disclosing a medical file with personal data in it to an external researcher would amount to a breach of professional secrecy and a violation of the rules on the protection of personal data.

The Polish legal system does not establish a specific procedure to be followed by a researcher seeking access to medical files. It does not determine, in particular, who is to cover the costs of the anonymisation. It should be concluded, therefore, that this question would be subject to an individual arrangement between the controller in possession of the relevant medical documentation and the research institution seeking access to it.

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 procedures will not change in Poland under the GDPR, as the rules for the collection of health data from health professionals and health institutions stem from a legal act (the Act on Patients' Rights and the Patient Rights Ombudsman) external to the data protection system. They are *leges speciales* comparing to general data protection rules, which – as mentioned earlier – is arguably reconcilable with the GDPR.

- **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.

In principle private databases could be developed upon specific consents of data subjects. It is rather unlikely, however, that a data subject would consent to revealing his/her personal data in a health database, even if the database is accessible only for research purposes. On the other hand, it would be extremely risky to contend that the producer of a private database can have a legitimate interest in disclosing personal information of the data subject without his or her consent (i.e. pursuant to Art. 7.f directive 95/46), as countervailing interests for fundamental rights and freedoms of the data subject – which require protection under Article 1.1 of this directive,

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

and which in practice imply pseudonimisation or anonymisation of the information in the database in the first place – seem particularly paramount in this setup.

In the scenario of establishing a private medical database based on information obtained by the producer from the institution in legitimate possession of medical records, the picture is ultimately similar: the only legally available option is to receive the medical data in an anonymised form, upon a separate contract concluded by the producer with the institution holding the medical documentation.

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 revised legal system does not effectively change the conditions applying to the setting up of a private data base.

- **PUBLIC DATABASES**

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

Public authorities are both permitted and obliged to share identifiable information on healthcare services and products according to the specific rules established by the Act on the System of Information in Healthcare. The interoperability of public healthcare databases is to allow for monitoring of public healthcare expenditure and for overseeing the provision of publicly funded healthcare. It should be technologically possible to export information contained in these databases to external databases (public or private) and the majority of the databases comprising the SIH provides for statistical modules containing anonymous information published by the authorities operating the databases. Yet, none of the public databases within the SIH has been established as a public research database available to external researchers.

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 effectively 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". [3]

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.

Processing of personal data would be permissible under Art. 89 GDPR in this scenario, assuming that all the rights of the data subject are respected accordingly, as the Polish legislator has not waived them as possible under Art. 89.2 or 89.3 GDPR.

2. Intensive Care Unit (ICU)

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

According to Polish law both prior and after the entry into force of the GDPR health data in the existing databases must be recognised as medical documentation to be covered by the professional secrecy, transferrable to the database of the AEGLE project only after anonymisation. When subsequently the AEGLE project processes the information anonymised in this way, it should be exempt from any obligations regarding data protection, of course as far as it does not process any information "relating to an identified or identifiable natural person". More specifically, data protection rules should not apply as long as the data received by the AEGLE project is anonymised and the project team cannot otherwise match it up with other information allowing for identification of the individuals to whom the health data refers.

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.

As the data coming from biobanks certainly concerns the state of health of the individuals, the information the AEGLE project seeks to re-use should be qualified as elements of medical documentation, which – pursuant to the Act on patients' rights and the Patient Rights Ombudsman – can be made accessible for the AEGLE project only after anonymisation. The anonymisation should be performed by biobanks, prior to disclosing the data to the AEGLE project (from the perspective of the project the data would be anonymised in this scenario). In this scenario,

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

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

however, the AEGLE project will not process personal data, either in the sense of Directive 95/46 or the GDPR. Hence none of their provisions should apply to the subsequent processing of the received 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