ISSN 2704-8012

European Journal of Privacy Law & Technologies

Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

PATIENTS AND PRIVACY: GDPR COMPLIANCE FOR HEALTHCARE ORGANISATIONS IN THE CZECH REPUBLIC *

Martin Šolc, Charles University Faculty of Law

Abstract:

At first sight, 25 May 2018 brought no revolution to Czech health care regarding data protection. The practice of the providers of health services related to medical records has already been aptly regulated by the Act on Health Services of 2011. Nevertheless, GDPR has caused several dilemmas, most importantly in the area of medical research and particularly biobanks. The paper focuses on selected questions related to GDPR compliance in Czech health care and medical research, outlining the answer to the question of what changed with GDPR and what it means to the relevant subjects.

Keyword: General Data Protection Regulation, compliance, health law, data protection in health care, the Czech Republic

Summary: 1. Introduction. – 2. Medical records under Czech law. – 2.1. The influence of GDPR on clinical practice. – 2.2. Problematic areas. – 3. Medical research and biobanks. – 3.1. Legal basis for the processing of personal data for scientific purposes. – 3.2. Further processing for scientific purposes. – 3.3. Processing of health data. – 3.4. Biobanks in the Czech Republic. – 4. Conclusion.

1. Introduction

There has been much debate on the practical effects of the General Data Protection Regulation [1] (hereinafter "GDPR") application in many sectors where the

* The paper was written with the support of the Charles University Grant Agency (GAUK) research project no. 910319 *"Legal Paradigm of Medical Research: Civil Liability for Death and Bodily Harm"*.

The author would also like to express his sincere gratitude for the invaluable consultations to Mgr. et Mgr. Anna Nevečeřalová and JUDr. Petr Šustek, Ph.D.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

personal data are processed. One of the more sensitive areas is health care where health-related data (which represent a special category of protected data under GDPR) are processed on a large scale. Nevertheless, it was precisely for this apparent necessity for the protection of patients' privacy that the data processing in health care has already been subjected to a relatively complex regulation before 25 May 2018 when GDPR became fully applicable. As a result, it is not always clear what new changes GDPR requires from Czech health services providers and health professionals. The article identifies the most important of these changes and outlines several problematic areas of data protection both in clinical practice and medical research (primarily related to the functioning of biobanks).

2. Medical records under Czech law

Medical records contain several categories of personal data that are subjected to special protection under Article 9 (1) of GDPR. From their very nature, medical records represent sets of data concerning health. However, they can also encompass genetic or biometric data. In some cases, there might also be present data concerning a person's sex life or sexual orientation. The medical records can also contain data revealing the patient's racial or ethnic origin. This rich mixture of personal data makes medical records extremely sensitive, requiring a high level of protection.

Since the provider of health services is obliged to keep medical records, the processing of the relevant data is necessary for compliance with a legal obligation to which the provider as a controller is subjected (Article 6 (1) (c) of GDRP). However, this sole reason would not suffice to legalise the processing of the above-outlined special categories of personal data. The processing of these data is only allowed since it is necessary for health purposes listed in Article 9 (2) (h), especially for the provision of health care.

2.1. The influence of GDPR on clinical practice

GDPR did not bring about any crucial change for Czech clinical practice. The general principles of data protection have been known to Czech law for many years [2]. Before May 2018, the keeping of medical records had already

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] See for example J. NAVRÁTIL ET AL., *GDPR pro praxi [GDPR for Practice]* (Plzeň 2018), 66-67.

been regulated by Act No. 372/2011 Coll., on Health Services and Conditions of Their Provision (hereinafter "Act on Health Services") and by Decree No. 98/2012 Coll., on Medical Records. The privacy rights of patients have been adequately protected by these regulations [3]. The area in which GDPR might prove more innovative – and more demanding – for Czech providers of health services is the protection of personal data of their employees. Another change following the applicability of GDPR was the limitation of some of the time periods for which certain types of medical records must be stored [4]. While this move somewhat alleviates the administrative burden borne by the providers of health services, its suitability from the perspective of patients' interests is apparently open for a discussion.

It needs to be noted, though, that the relatively high quality of patients' data protection in Czech national law did not have a very long tradition in the country. On the one hand, medical professionals have always been thinking about the necessity to keep their patient's secrets [5]. In this sense, medicine has been ahead of most of other professions regarding what we now call personal data protection. On the other hand, medical paternalism often led physicians to believe they know the best when, how, and to whom to reveal the information about their patients. In the Czech Republic, the patients' access to their own medical records was uncertain until about 2005. The significant improvement followed the ratification of the Convention on Human Rights and Biomedicine (hereinafter "Convention") in 2001. Article 10 of the Convention sets two basic rights regarding personal data in health care: everyone has the right to respect for private life in relation to information about his or her health as well as the right to know any information collected about his or her health [6]. Even though the minimum standards set by the Convention were considered almost self-evident in Western Europe, they represented a significant challenge for Czech health law of the time.

---

[3] See L. ŠIROKÁ-P. ŠUSTEK, Zdravotnická dokumentace [Medical Records], P. ŠUSTEK-T. HOLČAPEK (eds.), *Zdravotnické právo [Health Law]* (Praha 2016), 162-196.

[4] For example, the required time of storage of medical records in case of long-term inpatient care was limited from 40 to 20 years. Appendix 3 to Decree No. 98/2012 Coll., on Medical Records.

[5] Even the oldest known version of the Hippocratic Oath contains the promise to keep confidentiality: *"And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."* Hippocrates of Cos, *The Oath* (Loeb Classical Library) available at <https://www.loebclassics.com/view/hippocrates_cos-oath/1923/pb_LCL147.299.xml;jsessionid=0D172B139B8933CBD47CC1A575EBB4FE> accessed 10 January 2020.

[6] Nevertheless, the exercise of the latter right may be restricted by the law in the interests of the patient (the so-called therapeutic privilege). See M. ŠOLC, *Therapeutic Privilege as the Last Bastion of Paternalism?* in *Riv. Resp. med.*, 2019, 3, 399-403.

The remaining paternalism – directly inherited from the Socialist law – was still relatively strong and incompatible with the Convention's requirements. Since 1992, the obligation to keep medical records was explicitly imposed by the law, but the regulation only applied to private health care providers. The obligations applicable to all the providers (including the public ones) were set by Act No. 20/1966 Coll., on the Care for the Health of the People that did not explicitly mention medical records until August 2001. Even several years later, there were cases where hospitals attempted to deny the patients access to their own medical records [7]. By the late 2000s, the providers learnt to comply with the new requirements. The Act No. 20/1966 Coll. was replaced by Act on Health Services in 2012 which in its Section 65 guarantees the right to access to medical records to several groups of persons, including the patients themselves, the deceased's patients close persons, or the employees of the provider of health services in a necessary scope for the fulfilment of their duties.

Nevertheless, there are several new obligations that GDPR imposes on the providers in the position of controllers. Since the providers' core activities [8] consist in the processing of a large scale of special categories of data pursuant to Article 9 (see Article 37 (1) (c) of GDPR), they are obliged to designate a data protection officer *(DPO)*. This might prove challenging since the DPO should have a good understanding of both the area of data protection and the provision of health care, often including medical research [9]. It might be one of the reasons for which a provider of health services might choose to designate a team that will fulfil the tasks of DPO – in this case, though, there must still be designated a particular responsible natural person [10].

---

[7] See P. Šustek, *Two Decades of the Convention on Biomedicine: Has It Been Any Good?* (2018) 9 *Czech Yearbook of Public & Private International Law*, 262.

[8] The fact that the processing of personal data is one of the core activities of hospitals is aptly explained by the WP29: "*(...) 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.*" WP29, *Guidelines on Data Protection Officers ('DPOs')* (2016) 7.

[9] See J. Navratil et al. (fn 2), 63, 262-263; M. Nulicek-J. Donát-F. Nonnemann-B. Lichnovský-J. Tomíšek, *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář [GDPR. The General Data Protection Regulation. A Practical Commentary]* (Praha 2017), 339.

[10] See L. Suchánková, *Komentář k čl. 37 [Commentary to Article 37],* J. Pattynová-L. Suchánková-J. Černý et al., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světe. Komentář [General Data Protection Regulation (GDPR). Data and Privacy in a Digital World. A Commentary]* (Plzeň 2018), 291-292.

For a similar reason – because the providers process on a large scale special categories of data referred to in Article 9 (1) (see Article 35 (3) (b) of GDPR) – they are also obliged to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data *(Data Protection Impact Assessment, DPIA)*. On a general level, the DPIA is only required when the relevant processing operations are "*likely to result in a high risk*" [11]. The seriousness of the risk is assessed by the controller who in case of the serious risk danger also carries out the DPIA. Nevertheless, given the sensitivity of health data as well as the vulnerability of patients as data subjects, the processing of these data will be a typical example of processing requiring the DPIA [12]. While a similar procedure was already known to several European jurisdictions before GDPR (we can recall the *Privacy Impact Assessment* under English or French law), it was not present in Czech law [13]. The obligation to carry out the DPIA, however, only applies to bigger providers. Therefore, most physicians in private practice are exempted from the obligation [14]. This exemption also applies to other individual health professionals or lawyers and arguably other similar professions that have a legal duty of confidentiality, given that they process the data of a limited number of clients [15]. In the Czech Republic, the threshold is seen to be around 5.000 patients the provider has in care, while the average number of patients of a general practitioner is approximately 1.600 [16].

---

[11] See Article 35 (1) and Recital 91 of GDPR.

[12] A hospital processing of its patients' genetic and health data in a hospital information system is explicitly stated as an example of processing likely to require DPIA by the Data Protection Working Party WP29 in WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679* (2017), 11.

[13] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9), 312.

[14] Recital 91 of GDPR: *"The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."*

[15] See J. ČERNÝ, *Komentář k čl. 35 [Commentary to Article 35],* J. PATTYNOVÁ-L. SUCHÁNKOVÁ-J. ČERNÝ ET AL., *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světe. Komentář [General Data Protection Regulation (GDPR). Data and Privacy in a Digital World. A Commentary]* (Plzeň 2018), 273.

[16] See Appendix 2 to the draft document issued by the national authority data protection authority: Office for Personal Data Protection. "Data Protection Impact Assessment" Draft Version (2018) available at <https://www.uoou.cz/k-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385> accessed 10 January 2020.

2.2. Problematic areas

The most problematic areas concerning the data protection in clinical practice rather consist in the access to medical records of certain persons other than the patients and the health professionals. For example, a problem arose when the National Contact Point for eHealth [17] was established in summer of 2018 [18]. Initially, the existence of this information system significantly broadened the scope of persons having access to medical records [19]. In spring 2019, this scope was narrowed to the health services providers from other EU states via the respective national contact point. Nevertheless, it might be argued that the regulation is still lacking adequate safeguards.

From a certain perspective, the access of insurance companies to medical records is problematic in the opposite way. Every provider of health services is obliged to have liability insurance [20]. For the purposes of the investigation of a loss event, the insurance company needs to work with the data concerning the injured person's health condition or the cause of her or his death. However, according to Section 2864 of Act No. 89/2012 Coll., the Civil Code (hereinafter "Civil Code"), the insurer is only allowed to ascertain such data if they have been granted consent to do so by the injured person or another person entitled to grant the consent. The same rule applies to access to medical records.

The injured party usually grants the consent – it is in their best interest to ensure that the insurance company will pay their compensation. Nevertheless, if the injured person refuses to grant the consent, the insurance company cannot investigate the case and cover the costs. For the insured provider of health services, this might be a very difficult situation: they have to compensate the injured person from their own sources without hope to have the costs covered by insurance. It is not very fortunate for insurance companies as well since they cannot really promise the insured persons their protection in all cases.

GDPR is of little help in this respect. Article 9 (2) does not provide the insurers with any legal basis for ascertaining health-related data of the injured persons. The only option is to ascertain and process the data for the defence against legal claims (Article 9 (2) (f) of GDPR). However, this is only applica-

[17] In Czech original: *Národní kontaktní místo pro elektronické zdravotnictví*.

[18] From the legislative perspective, it was established by adding the new Section 69a to Act on Health Services.

[19] See J. MACH-A. BURIÁNEK-D. ZÁLESKÁ-M. MÁCA-B. VRÁBLOVÁ, *Zákon o zdravotních službách. Zákon o specifických zdravotních službách. Praktický komentář. [Act on Health Services. And on Specific Health Services. A Practical Commentary]* (Praha 2018) 281-282; J. NAVRÁTIL ET AL. (fn 2) 163.

[20] See Section 45 (2) (n) of Act on Health Services.

ble if the litigation already started and the insurance company joined it as an intervenor. It does not help the insured providers with their uncertainty very much. Furthermore, it excludes the possibility of out of court settlement.

A somewhat related problem is connected to private health insurance. While there is a system of mandatory public health insurance in the Czech Republic, many foreigners are only insured privately. These patients can simply walk away from the health facility without paying, and it is virtually impossible for the provider to enforce the patient's duty to pay for the provided services since they have no legal basis for using the patient's personal data.

3. Medical research and biobanks

The processing of personal data for the purposes of medical research is rather complicated. It is necessary to find out whether there is any legal basis for this processing other than the data subject's consent. Furthermore, we will identify the conditions of further processing for scientific purposes if the data were collected for some other purpose. Then, we will focus on the special legal basis for the processing of health data. Finally, we will briefly analyse the contemporary situation of Czech biobanks.

3.1. Legal basis for the processing of personal data for scientific purposes

If personal data are to be processed without their subject's consent, there arises an important question of whether the medical research is a task carried out in the public interest in the sense of Article 6 (1) (e) of GDPR. If the answer were affirmative, the processing of data would be possible without consent given that it has a basis in Union or Member State law [21]. Nevertheless, this criterion is primarily applicable to public authorities [22]. In the context of health care, GDPR explicitly mentions the processing carried out with the purpose of public health protection or the management of health care services by subjects such as professional associations [23]. It is not clear whether the medical research carried out by research institutions – including the public ones – can reasonably fit into this category. This uncertainty is especially relevant with regard to clinical stud-

[21] See Recital 45 of GDPR.

[22] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 130.

[23] Recital 45 of GDPR.

ies of new medicinal products or medical devices that might be understood as a mixture of public and private interest.

Alternatively, it is feasible that the processing for research purposes is necessary for the purposes of the legitimate interests pursued by the controller or by a third party according to Article 6 (1) (f) of GDPR. Under Directive 95/46/EC that was later repealed by GDPR, the Article 29 Working Party (WP29) had come to the conclusion that scientific or research purposes can constitute a legitimate interest [24]. While the legitimate interest is one of the most flexible of the legal grounds for data processing [25], it is not unlimited. It should not apply to the processing by public authorities in the performance of their tasks. In the case of other controllers, the legitimate interest can be given especially if "*there is a relevant and appropriate relationship between the data subject and the controller*" [26]. The practice would need to clarify under what circumstances the relationship between the provider of health services and the patient could be relevant and appropriate for this legal basis to be applied. Furthermore, the legitimate interests criterion always entails a balancing test since the processing is not allowed if the interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject. This could especially happen "*where personal data are processed in circumstances where data subjects do not reasonably expect further processing*" [27].

Therefore, the processing of personal data for research purposes without consent might be possible as constituting legitimate interest of the controller. However, the research institutions need to be very careful in each case [28]. It is commendable that the processing of personal data in research is based on consent. Even in that case, it remains to be clarified how specific the consent must be.

3.2. Further processing for scientific purposes

Another problem is the further processing of personal data for a purpose other than for which they were collected (see Article 6 (4) of GDPR). We can imagine a situation when the patient consented to the processing of his or her per-

[24] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (2014), 24-25.

[25] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 131.

[26] Recital 47 of GDPR.

[27] *Ibidem*.

[28] See also G. MALDOFF, *How GDPR changes the rules for research?* (19 April 2016) *The International Association of Privacy Professionals* available at <https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/> accessed 27 January 2020.

sonal data in the context of the provision of health care, but the data are later used in health research. There are two possible legal bases for this processing. The first one is the additional consent granted before the processing of data for the new purpose. The second legal basis is the compatibility of the new and the original purposes. The compatibility shall be ascertained by the controller. They should take into account several aspects, for example, any link between the original and the new purposes, the context of the data collection, the stricter protection of the data pursuant Article 9 of GDPR, the possible consequences of the further processing, or the existence of appropriate safeguards (e.g. pseudonymisation).

Nevertheless, according to Article 5 (1) (b) of GDPR, *"further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes"*. Also, Recital 50 of GDPR states that the *"[f]urther processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations"*. For this reason, further processing for scientific purposes should be legal in most cases even without consent. However, it is still possible that sometimes the difference between the original and the new purpose will be so significant that the purposes will be considered incompatible. The controller should, therefore, carry out the test of compatibility, which is burdensome from the perspective of administrative costs.

3.3. Processing of health data

When health data are concerned, the processing also needs to have a legal basis under Article 9 of GDPR. Explicit consent of the data subject is, of course, one of these legal grounds. Another possibility is to be found in Article 9 (2) (j) on which the processing can be based if it is necessary for, inter alia, scientific research purposes, it is subject to safeguards set by Article 89 (1), and it is 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. This provision in conjunction with Article 6 (1) (f) arguably represents a sufficient legal basis for the processing of health data for scientific purposes without the consent of the data subject.

3.4. Biobanks in the Czech Republic

It is problematic that some of Czech health data registers are not regulated by any law or decree. However, there is also a broader question that threatens to undermine the processing of health data in the research context in the country. Under Czech law, the use of biological material for research purposes does not require the patient's consent if in the course of its use there are not used data that would make it possible to identify the patient or the deceased person (Section 81 (4) (a) of Act on Health Services). This requirement is crucial for biobanks (repositories that process, store, and distribute biospecimens and associated data for the use in research and clinical practice [29]). An important feature of biobanks is their ability to provide samples for a variety of future research purposes as opposed to traditional sample collections which have only been collecting each sample for a specific research need that was defined in advance [30].

Biobanks often provide samples to foreign researchers. The patient is known under a specific code to which the data are connected (clinical information, genetic data, lifestyle data, etc.). It is a usual practice that researchers ask for the information on the development of the patient's condition. This requires that the controller is still able to connect the code with the particular patient.

Anonymisation as a process represents the data processing, but the resulting anonymised data are not considered personal data and therefore are not protected by GDPR or national law. That is because anonymisation is irreversible; once the data are anonymised, the natural person cannot be directly or indirectly identified by the controller or by another person with the use of *"all the means reasonably likely to be used"* [31]. If it is still possible to identify the person by any reasonably foreseeable means, the data were not anonymised. And there is no doubt that as a rule, the data in biobanks can be used to identify the person. Therefore, these data are "merely" pseudonymised and cannot be considered anonymised.

The pseudonymisation of data would not necessarily be a problem if the data could simply be used under the legitimate interests clause (the above-analysed Article 6 (1) (f) of GDPR). From the sole perspective of GDPR, the data collected with the consent as a part of a research biobank can be used by the biobank administrators for other forms of scientific research without additional consent [32].

---

[29] See Y. G. De Souza-J. S. Greenspan, *Biobanking Past, Present and Future: Responsibilities and Benefits* (2013) 27 (3) *AIDS*, 303.

[30] See S. Biopankit, *What is a Biobank?* available at <https://www.biopankki.fi/en/what-is-a-biobank/> accessed 10 January 2020.

[31] Recital 26 of GDPR. See also WP29, *Opinion 05/2014 on Anonymisation Techniques* (2014) 5.

[32] See B.A. Simell-O. M. Törnwall-I. Hämäläinen-H.E. Wichmann-G. Anton-P. Bren-

However, the fact that biobanks contain health material means that the processing must be based on a Member State law as required by Article 9 (2) (j) of GDPR.

Therefore, the crucial question is whether the condition of the impossibility to identify the patient under Czech law means anonymisation or pseudonymisation. If Czech law required anonymisation, most of the activity of biobanks would not be possible since it would not be based on a Member State law. The specific purposes of future sample processing in a biobank cannot be foreseen in the time of the consent. For this reason, the consent can hardly be specific enough to meet the GDPR standard.

If interpreted extensively, anonymisation would not be possible in any human tissue since every tissue contains DNA. This is even more evident given that in their decision making, the controllers should take into account the possible future development of the possibilities of identification of persons [33]. Even the tissue samples that are relatively safe from identification today can be much more easily identified in the future with the development of science and the increasing popularity of commercial DNA testing. We believe that this fact only strengthens the argument for the pseudonymisation interpretation of the above-discussed Czech legal requirement.

4. Conclusion

Following the ratification of the Convention on Human Rights and Biomedicine in 2001, Czech health law made significant progress in securing the protection of patients' privacy. For this reason, GDPR did not bring about much change regarding the keeping of medical records. Nevertheless, it imposed several new obligations on the providers of health services such as the duty to designate a data protection officer or to carry out the data protection impact assessment. Furthermore, there remain several problematic areas, including the regulation of the access of insurance companies to medical records.

Processing of health data without consent for the purposes of medical research can be arguably based on Article 6 (1) (f) (legitimate interests) in conjunction with Article 9 (2) (j) (scientific research) of GDPR. Further processing

---

NAN-L. BOUVARD-N. SLIMANI-A. MOSKAL-M. GUNTER-K. ZATLOUKAL-J.T. MINION-S. SOINI-M.T. MAYRHOFER-M.J. MURTAGH-G.J. VAN OMMEN-M. JOHANSSON-M. PEROLA, *Transnational access to large prospective cohorts in Europe: Current trends and unmet needs* (2019) 49 *New Biotechnology*, 98-103 as cited in European Parliament. Panel for the Future of Science and Technology, "How the General Data Protection Regulation changes the rules for scientific research" available at <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf> accessed 26 January 2020.

[33] See M. NULÍČEK-J. DONÁT-F. NONNEMANN-B. LICHNOVSKÝ-J. TOMÍŠEK (fn 9) 83-84.

needs to be subjected to the test of compatibility of the original and the new purposes of processing (even though the new purpose should be considered compatible if it consists in scientific research). It is primarily the national law that makes the legality of standard practices of health data processing in biobanks uncertain. According to national law, the patient's consent for the use of biological material for research purposes is not required only if it is not possible to identify the patient from the used data. As a rule, the data in the biobanks are pseudonymised but not anonymised. While the situation is far from clear, we argue for the interpretation of the said legal requirement in the sense of pseudonymisation, so the functioning of biobanks is not threatened.