Medical registries in perspective of the new EU's legal framework of personal data protection - selected issues

DOI: 10.7365 / JHPOR.2016.1.1

Authors:

Monika Krasińska[1]

1- Cardinal Stefan Wyszyński University in Warsaw

Keywords:

medical registriers, processing of personal data, special categories of personal data

Abstract

Keeping medical registries is inextricably linked with the processing of personal data, which often belong to the most sensitive sphere of privacy of every individual. Creating a comprehensive and complete legislation in this area is a guarantee of proper protection of the privacy and dignity of the patient, and is a part of the optimal model of protection of personal data representing the content of the registers, which is guaranteed both at the level of constitutional and international law. The creation of appropriate legal mechanisms must also be accompanied by a friendly technical and organizational environment. Lack of financial resources to ensure the security of data stored in the medical records may result in the risk of data leaks, unauthorized access to data, or using data for the wrongpurposes. In view of the reform of the EU data protection law the above-mentioned circumstances must be a subject of in-depth analysis.

Genesis and consequences of changes in the European regulations on personal data protection

Directive of the European Parliament and Council of 24th October 1995 (95/46/EC) on protection of physical persons and in the scope of personal data processing and their free movement has imposed on the members of the European Union an obligation to respect the core rights of the individual in the process of free movement of goods, persons and capital within the functioning internal market. Despite the fact that, by assumption, the Directive was to be an act, consolidating the standards of data protection in all the Member States of the European Union, a multiplicity of various practices was growing in the area of personal data protection law implementation. The legal solutions, imposed by the Directive, did not, moreover, respond to the progressing technological development, what constituted obstacles in data movement, not conductive for the economic development within the European Economic Area (EEA). It was then necessary to construct such legislative solutions which would enable an implementation of tools, maximally tailored to the technological development, in particular, digitalisation and globalisation challenges, including transfrontier services. The works on unification of the personal data protection law, which have been underway since 2012, have just been completed.

On the 4th May 2016, in **the Official Journal of the European Union, L 119, the Regulation of the European Parliament and Council (EU), 2016/679 of 27th April 2016 was published. This Regulation applies to the protection of natural persons with regard to the processing of personal data and to the free movement of such data, as well as it repeals 95/46/EC Directive** (general regulation on personal data protection), further called "the Regulation". The Regulation entered into force on 24th May 2016 and **shall become effective from 25th May 2018.**

This Regulation creates a new model of approach towards the issue of personal data protection, both in private and public sector. Some of the introduced amendments may even represent the nature, unknown to the to-date's Union's law. On one hand, this Regulation grants physical persons with new rights, increasing the level of their protection, while imposing new tasks and obligations, both on entrepreneurs and on the public administration on the other. In any event, it is necessary to start preparations to implement these new provisions.. The scale of introduced changes will undoubtedly require an implementation of new technological tools or modifications of the present IT solutions.

The Regulation shall be applied directly, what means that, in case of any non-compliance of the provisions of the national law with the provisions of the Regulation, then any data subject shall have the right to demand direct application of the provisions of this Regulation and enforce appropriate claims against infringers of its protection rights.

This Regulation focuses on more effective protection of the privacy of physical persons, as well as on higher accountability of data administrators, both in the context of the quality of processed data (their veracity and correctness in substance), their volume (the principle of proportionality), processing periodicity or, eventually, on providing more transparency to the process, both from the level of the administrator alone (self-control with support of personal data inspectors) and the data subjects (information obligations, the right to request removal of personal data, the right to be forgotten, etc.).

In order to strengthen the rights of data subjects, new mechanisms have been introduced, thus far unprecedented in the Polish law of data protection, including, among others: **codes of conduct**, enabling real-time monitoring of data processing and the growing improvement of their quality or the **mechanisms of certification with accredited certifying products**[1].

Children have been given special protection status, as subjects less aware of their rights and of possible threats, associated with data processing[2].

Data administrators shall also be obliged to a more exhaustive analysis of "the right to be forgotten", the right of data portability, as well as the right to obtain their copy. Keeping a registry of data processing operations instead of the registry of personal data files will, in turn, serve informalisation of to-date's notification procedures of personal data files to shift the centre of gravity from the supervision of data processing towards data administrator's self-control, carried out, for the most part, by the in-house inspector of personal data protection.

The unquestionably extended obligations of data administrator are simultaneously accompanied by extensive rights of data subjects, who will acquire the right to enter the environment of their data processing in a broader perspective. And so, both at the level of data acquisition and the level of the process continuation, any person, whose data are processed, will be able to evaluate the correctness of operations on his/her data, as well as the correctness of actions, undertaken by the subjects, collaborating with the data administrator, including the right of evaluation of a given subject, while reporting his/her doubts at a contact point which will, in fact, become the person of personal data protection inspector, designated by the data administrator. In case when an infringement occurs, causing a high risk of breaching the rights or freedom of physical persons, the data administrator will immediately have to advise the affected person about such an incident, while keeping a register of breaches to coordinate the politics of data processing in real time and eliminate the risk of subsequent breaches.

Therefore, the provisions of the discussed general Regulation on personal data protection have to be incorporated into the review of to-date's national regulations, concerning privacy protection. This query takes on particular importance in case when the processed data are of sensitive type, such as data in medical records of patients. In such cases, there is a significant interference in the right for privacy of man and such interference may proceed without simultaneous, special warranty for protection of these data. This regulation has narrowed the obligation of responsibility for sensitive personal data processing. Processing of data from this category carries the risk of suffering far-reaching consequences in case of failure in performing required obligations by data administrator. There are also legal arrangements in the regulation, which indicate a need of restructuring of the current provisions, shaping the frames of permitted interference in the information autonomy of the individual.

Medical registries and the principle of legality

The discussion, lasting in Poland for many years and concerning the use of data, contained in medical registry resources, has been accompanied by a fairly consequent position of the personal data protection authority which, since the very beginning of its existence, has been emphasising the problem with the lack of any statutory regulations, which would address this issue. Medical registries have for years not been inventoried, while their practical use has not been regulated by any pre-defined legal frames. Then they were constructed on the basis of implementing acts, what - first of all - did not comply with constitutional requirements and violated the rules of personal data protection. Indeed, pursuant to art. 27 section 2 item 2 of the Act on personal data protection[3], health status data processing is allowed and a specific provision of another act allows for processing of such data without consent of the data subject and provides full guarantee of their protection. The principle of legalism was not sufficiently expressed in the construction of art. 20 section 1, pursuant to art. 19 section 1 of the Act on the information system in health care[4], what was confirmed by the Constitutional Court in its judgement of 18th December 2014[5]. The Court pointed out that, although the goals of medical registries and their creation may be considered necessary in a democratic state ruled by law - in acc. with art. 51 section 2 of the Constitution - both monitoring of demands for medical care services, addressing the health status of the citizens, and the conduct of effective health policy and implementation of healthcare programmes, serve the ensurance of public safety and health (art. 31 section 3 of the Constitution) - still the definition in the Act of the substantial scope of the medical registries and of the type of data contained in them does not meet the requirements for the constitutional limitation of information autonomy.

However, despite the adjustment of the questioned regulations to the provisions of the above-mentioned Judgement, still no appropriate guarantees have been ensured for personal data protection in the scope of data, processed in the National Cancer Registry. Namely, neither the scope nor the type of data, processed in this Registry, has been indicated. In a project, presented for an opinion of the General Inspector of Personal Data Protection [6], instead of the statutorily required catalogue of data, approved for processing, the project refers this issue to the pattern of Cancer Notification Form, defined in the Act, issued on the basis of Art. 31 of the Act on public statistics, i.e., another executive act[7]. Such a proposal leads then to a specific legalisation of the executive regulations to the act on public statistics, as a legal basis for

processing of sensitive data[8]. Moreover, an acceptance of presented proposal would mean that not the Minister of Health (what is guaranteed by the act on the information system in health care) but the Prime Minister would decide on the scope and type of data, while drafting the pattern of cancer notification card[9]. Such solutions do not lead to construction of proper data protection standards and may raise doubts from the level of the provisions of the Regulation on personal data protection, which emphasises that exceptions from sensitive data processing prohibition are possible unless the EU's law assumes specific, appropriate measures, protecting the fundamental rights and personal data of physical persons (recital 53 and art. 9 section 2 item b).

Medical registries vs. new definitions

Although the provisions of the regulation repeat, to a large extent, the premises of legal processing of sensitive data from 95/46/EC Directive, they create entirely novel ideas in the definition zone. It is of basic significance for evaluation of the to-date's scope of data, identified as personal data and contained in medical registries. An example may be the definition of **genetic data** (art. 4 item 13 of the Regulation) or of the **biometric data** (art. 4 item 14 of the Regulation). The recognition of biometric data as sensitive data is a novel approach. In this matter, also the issue of legality of using the biometric data in the sphere of IT system safety management requires consideration, as well as an establishment of appropriate legal basis for the purpose of using sensitive data. Moreover, it is not only a problem, insufficiently resolved from the level of medical information management but, in general, an issue on which the Ministry of Labour itself has yet to come down on one side of or the other. The regulation of using biometry by employers is even more significant as the acquisition of this category of information constitutes a particular interference into the right of the employee's privacy.

In addition, the Regulation defines the term of **co-administrator**, not yet implemented in the Polish Law[10]. A review of the status of the entities, which run medical registries, will also be important from the point of view of the provisions of the above-mentioned Act, creating a broader model of accountability but also of responsibility of an entity, which acts by order of data administrator and occurs as a **processing entity**.

The procedure of processing data, contained in medical registries, serves clearly defined objectives and is, by definition, carried out in an automatic way. Undoubtedly, the compilation of definite personal data contributes to the implementation of the procedure for the purpose of an analysis of prognosis of health status aspects, what will often lead to certain **profiling** of physical persons. However, in such situation, the EU's legislator imposes the use of appropriate legal mechanisms for the protection of rights of profiled persons and for limitation of automated decision-making in individual cases and, first of all, the ensurance of full transparency of the processing procedure, carried out in such a way, for the data subject. Although the regulations, introduced in the Act on the information system in health care, ensure meeting the postulate for data processing transparency[11], still, they will have to be revised and updated in the light of changes in the scope of the contents of the right to information, resulting directly from the Regulation.

Responsibility for data protection law infringement

The Regulation moves away from the to-date's model of responsibility for infringements in the personal data protection zone. The Polish Act on personal data protection does not include any regulations on the principles of financial responsibility, regarding the administrator who would breach the rules of data processing. The General Inspector of Personal Data Protection may issue exclusively administrative decisions, ordering to use reasonable measures to remove the infringements, while their execution proceeds in line with administrative regulations. In case when an administrative decision is not implemented, the authority of personal data protection may notify request law enforcement bodies about committed offence and then verify, as an involved party, the appropriateness of the taken position in due course and by separate approach.

The issue of data administrator's responsibility has been regulated in various ways in particular countries of the European Union, becoming one of the major elements of debate on new legal frames for personal data protection. Therefore the regulations have been harmonised. And so, any person who has suffered material or non-material damage in result of infringement of teh Regulation provisions, has the right to receive due **compensation** from the data administrator or from the data processing entity. Moreover, every supervising authority (the authority of personal data protection) has acquired the right to impose **administrative financial penalties**, the amount of which may reach 20 million Euro and, in case of a business - up to 4% of its total, annual world turnover from the previous fiscal year.

Summary

The actual social changes, inspired mainly by technological developments and the impact of globalisation, impose a new approach to personal data protection. The scale of personal data acquisition, exchange and processing has undergone irrevocable changes, while data themselves have become the primary value in the development of digital economy in particular countries. In consequence, the risks, which are associated with data processing procedures, have also increased. In order to minimise them on normative basis, new, more stable and coherent frames have been introduced for personal data protection - provided by the discussed Regulation on data protection.

It should be taken into account that, in case of personal data, associated with health condition and accumulated in various IT systems, an evaluation of the processing procedure should be carried out at the earliest stage of their design and construction, so that only legal - and no IT solutions - decided about the final shape of data management procedures. Whereas, the act of executive character and even more the internal regulations of data administrator, may not always be appropriate for providing optimal data protection guaranties.

Personal data processing must not always be associated with the necessity of data identification. The periods of data retention in particular systems and registries should clearly be defined in order to eliminate the processing of data, which are either unnecessary for the implementation of planned objectives or used in not precisely drawn objectives by poorly defined subjects/groups of subjects. The Regulation takes a special account of the necessity of previous estimation of the results and effects of any project, planned for personal data protection and provides criteria for such estimation.

Although the currently valid Polish regulations extensively control the matter of personal data in medical registries, it still does not mean that the solutions, proposed in these regulations, fully reflect the principles of personal data protection, as set out by the standards of the Regulation. Many entities, which carry out tasks related to medical registries, give clear signals about the lack means to ensure basic principles of sensitive data protection, adjusted to currently valid regulations. The entities demonstrate a high degree of uncertainty and anxiety, regarding the implementation of the EU's regulations. It seems that this issue should therefore encourage a debate on the state of preparedness for implementation of the new personal data protection frames, not only with regards to medical registries but, in general, in the entire health care sector.

References

1. Section 5 Regulations
2. Art. 8 Regulations
3. The Act of 29th August 1997 (Journal of Laws from 2011, item 2135, as amended).
4. The Act of 28th April 2011 (Journal of Laws No. 113, item 657, as amended)
5. Judgement of the Constitutional Court of 18th December 2014, ref. No. K 33/13
6. http://legislacja.rcl.gov.pl/projekt/12280402/katalog/12330348
7. The Act of 29th August 1995 (Journal of Laws No. 2012, item 591, as amended)
8. Position of the General Inspector of Personal Data Protection of 13th January 2016, ref. No. DOLIS-033-6/16/TG/1698
9. A similar position was expressed by the General Inspector of Personal Data Protection in the Opinion of 19th April (ref. No. DOLIS-033-94/16/TG/32024) on the draft of the regulation of the Council of Ministers on the programme of statistical studies of public statistics for the year 2017.
10. The concept, introduced by the Act on the state's aid in upbringing of children, see Art. 38, should be recognised as a totally failed attempt in this scope and directly breaching the provisions of the discussed Regulation.
11. Pursuant to art. 19 section 9 of the Act on the information system in health care , the entity, which runs a registry, defined in the provisions, issued in line with art. 20 section 1, shall be obliged, within 30 days from the date when personal data processing procedure is commenced, to notify every person, whom the processed data concern and whose data are processed in the registry about:
1) the address of its registered seat and its full name;
2) the purpose, scope and mode of processing of the data relating to the person;
3) the right of access to data with a possibility of their revision;
4) the categories of recipients to whom the data from the registry are disclosed;
5) the obligation or the lack of obligation to inform about the data, which are processed in the registry and, if such an obligation is valid, about its legal basis.