Dr Artur Romaszewski
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems
Dr hab. Wojciech Trąbka
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems

The role and responsibilities of data controllers and processors in health care units in the light of the act on personal data protection and the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

All health care entities are preparing to introduce medical e-filing system and, consequently, to implement applications that are dedicated to such purpose. Thus, an opportunity emerged to look through the current documents that are related to personal data processing and are required by law. At the beginning of 2015 new regulations regarding the protection of personal data came into force and it is probable that in 2016 the European Union will implement a regulation on personal data protection – a proposal of the European Commission and the European Parliament[1] that will replace the EU Directive 95/46/EC on the protection of personal data. [2]

The new regulations are going to introduce several changes as regards the organization of health care entities. At present, after the introduction of the changes in the act on personal data protection, some of them are optional and the managers of the entities are not obliged to implement them. The situation will change when EU regulations come into force. Then, the regulations concerning, among other issues, the appointment of Information Security

[1] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)http://giodo.gov.pl/560/id_art/4503/j/pl/
[2] http://www.giodo.gov.pl/568/id_art/603/j/pl/

Controllers in health care entities who would meet legally defined criteria, are going to be obligatory.

The regulations regarding data protection are considered insufficient in relation to personal data. The current provisions of the act on personal data protection in Poland provide several legal sanctions for disrespecting the rules. However, the EU regulation provides for severe financial sanctions when the provisions of the regulation are not implemented. That refers particularly to the commitments of health care entities to implement adequate procedures that are required when processing personal data, including the ones that concern patient's health data, i.e. sensitive data. One of the assumptions of the reform is to impose "effective, proportionate and dissuasive" administrative sanctions against anyone who will not comply with the obligations laid down in the regulation. The supervisory authority (independent and impartial) will be entitled to impose at least one of the following sanctions: a warning in writing in cases of first and non-intentional non-compliance, regular periodic audits, a fine up to 100 000 000 EUR or up to 5% of the annual turnover[3] in case of an enterprise, whichever is higher[4].

Significant changes to the Act on personal data protection were introduced to the Polish legal system in the Act of 7 November 2014 on facilitation of performance of economic activity.[5] The changes have been in force since 1 January 2015 and regard mainly the functioning of Information Security Controllers in the entities and the issue of data transfer beyond the European Economic Area.

The EU regulation defines the notion of the controller who, as in the Act on personal data protection is either a natural or legal person, a public body, an organizational structure or any other entity that can independently or jointly with other entities (joint controllers) determine the purposes, conditions and means of the processing of personal data

[3] Amendment 188, article 79 (2a), Legislative resolution of the European Parliament of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

[4] BLOG PROFESJONALNIE O OCHRONIE DANYCH OSOBOWYCH - J Bardadyn - Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/

[5] Journal of Laws, 2014, item 1662

The article will discuss the most significant legal regulations and EU proposals for regulations relating to the functioning of data controller as the entity responsible for the purposes and means of personal data processing in health care units.

Specificity of medical data and health care information system

When analyzing the issue of personal data protection in a health care system, one should consider both the specific character of medical data (which are personal and often sensitive data) and a significant number of entities that are entitled to collect and process medical data as well as the even more numerous group of entities that have the right to access such data. The entities processing medical data form a diversified group as regards legal and organizational aspects as well as their size. Large hospitals, outpatient centres, medical centres and private practices have to collect, process, transmit and receive data. Another factor that influences the security of data is the significant number of potential system users that have different computer skills and experience. Moreover, the environment in which information systems are functioning require prompt and non-standard operations of access to medical data. The above issues and the specific features regarding the processing of medical data constitute a challenge when it comes to the implementation of the new legal regulations relating to personal data processing.

Implementation of appropriate technical and organizational measures

The provisions of law impose on the data controller and processor[6] the responsibility to implement appropriate technical and organizational measures to ensure security level adequate to the risk represented to processing, with the consideration of the results of data

[6] *Processor* - Where processing is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures Amendment 121, Proposal for a regulation of the European Parliament of 12 March 2014, article 26 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

protection impact assessment, having regard to the state of the art and the costs of their implementation.

Technical and organizational means that ensure data security include:

a) the assurance that personal data can be accessed only by authorized personnel for legally authorized purposes**;**
b) the protection of personal data stored or transmission against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure;
c) the implementation of a security policy with respect to the processing of personal data[7].

The state of the art to be implemented should ensure

a) the ability to ensure that the integrity of the personal data is validated;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services.(e.g. blackouts, Internet system failures);
d) in the case of sensitive personal data processing additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;
e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.

7 Amendment 124, Proposal for a regulation of the European Parliament of 12 March 2014, article 26 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor implement, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, appropriate and proportionate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject . Data protection by design has particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment, the results are taken into account when developing those measures and procedures**.** The controller ensures that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected**,** retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data[8].

Medical data – specific risk – predicted impact assessment

In the cases when data processing involves special risk as regards the rights and freedoms of a data subject due to their character, range and purposes, data controller or processor conduct personal data processing impact assessment.

Specific risk is involved with the operations that concern:

a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analyzing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behavior, which is based on automated processing and on which measures are based that

[8] Amendment 118, Proposal for a regulation of the European Parliament of 12 March 2014, article 23 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

produce legal effects concerning the individual or significantly affect the individual (e.g. insurance purposes);

b) processing the information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale (e.g. the health data processed by the NFZ – National Health Fund)

The data processing impact assessment includes at least:

- the assessment of risk to the rights and freedoms of data subjects,
- the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The personal data protection impact assessment should take into account the entire lifecycle management of personal data from collection to processing to deletion, and describe in detail processing envisaged, the risks to the rights and freedoms of data subjects, measures envisaged to mitigate the risks, safeguards, security measures and mechanisms to comply with the Regulation .

Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited[9]..

Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable

[9] Amendment 44, Proposal for a regulation of the European Parliament of 12 March 2014, Recital 71 a (new) on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

data management framework and by following it up with a comprehensive compliance mechanism[10].

Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the data protection officer or the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with the Regulation, and to make proposals to remedy such situation. Data controllers should conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. The reviews should demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance[11].

Risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly[12].

Following the evaluation of the risks, the controller and processor take measures:

-
- to protect personal data against accidental or unlawful destruction or accidental loss and,
- to prevent the data against any other forms of unlawful processing, particularly unauthorized access, disclosure or alteration.

At the time of the determination of the purposes and means for processing and at the time of the processing itself, the controller, having regard to current technical knowledge and

[10] Amendment 45, Proposal for a regulation, Recital 71 b (new), European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

[11] Amendment 48, Proposal for a regulation, Recital 74 a (new), European Parliament legislaltive resolution of 12 March 2014on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

[12] Article 32a, Legislative resolution of the European Parliament of 12 March 2014 on the proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

the implementation costs, implements appropriate and proportionate technical and organizational measures and procedures in such a way that the processing meets the requirements of the Regulation and ensures the protection of the rights of the data subject.

The controller is only burdened with measures that are proportionate to the risk of data processing reflected by the nature of the personal data to be processed.

The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself.

The controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimization and purpose limitation[13].

Undoubtedly – when a health care unit complies with the legal criteria of the Regulation - the most significant organizational problem that the managers will face is the consideration of the possibility or necessity to fit the Information Security Controller into the organizational structure.

Despite the fact that such post is not a new one – it existed in the structure of numerous health care institutions – its role has been significantly changed since the beginning of 2015.

Information Security Controller – data protection officer

The provisions of law impose on the data controller several responsibilities regarding data security, documentation concerning methods of data processing and appropriate

[13] Amendment 37, Proposal for a regulation, Recital 61, European Parliament legislative resolution of 12 March 2014 for a proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

technical and organizational measures to ensure security. The measures must be appropriate to the risks and the category of data under protection; they particularly should protect the data against unauthorized disclosure, theft, unlawful processing and alterations, damage or destruction[14].

The controller must make decision whether he will take the above responsibilities on his own or will appoint an Information Security Controller (ISC) . The regulations state clearly that the appointment of ISC is optional[15]. Alternatively, all tasks imposed by law on the data controller can be conducted solely by the data controller. In the case when ISC is not appointed, it is the responsibility of the data controller to conduct the tasks listed above except for the obligation to prepare reports to the personal data controller and to conduct a registry of personal data (Fig.1)

The issue of appointing ISC is treated differently in the Resolution. In the EU regulations ISC is referred to as a data protection officer.

The controller and processor appoint a data protection officer in every case when:

a) the processing is carried out in the public sector, or
b) in the private sector when processing relates to more than 5000 data subjects within 12 months irrespectively of the size of the enterprise, or where data processing is the core activity of the enterprise. When establishing whether data about a large number of data subjects are processed, archived data that is restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account,
c) the processing concerns sensitive data or when processing operations require regular and systematic monitoring[16]

[14] Art. 36. Act of 29 August 1997 on personal data protection (Journal of Laws, 1997, No.133, item 883
[15] 883 Art. 36a, Act of 29 August 1997 on personal data protection (Journal of Laws, 1997, No.133, item 883

[16] Art. 35 of the Resolution, Amendment 49, Proposal for the resolution, Recital 75, European Parliament legislative resolution of 12 March 2014 2014 on the proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

The role and responsibilities of ISC in health care units will be discussed in detail in a separate paper.

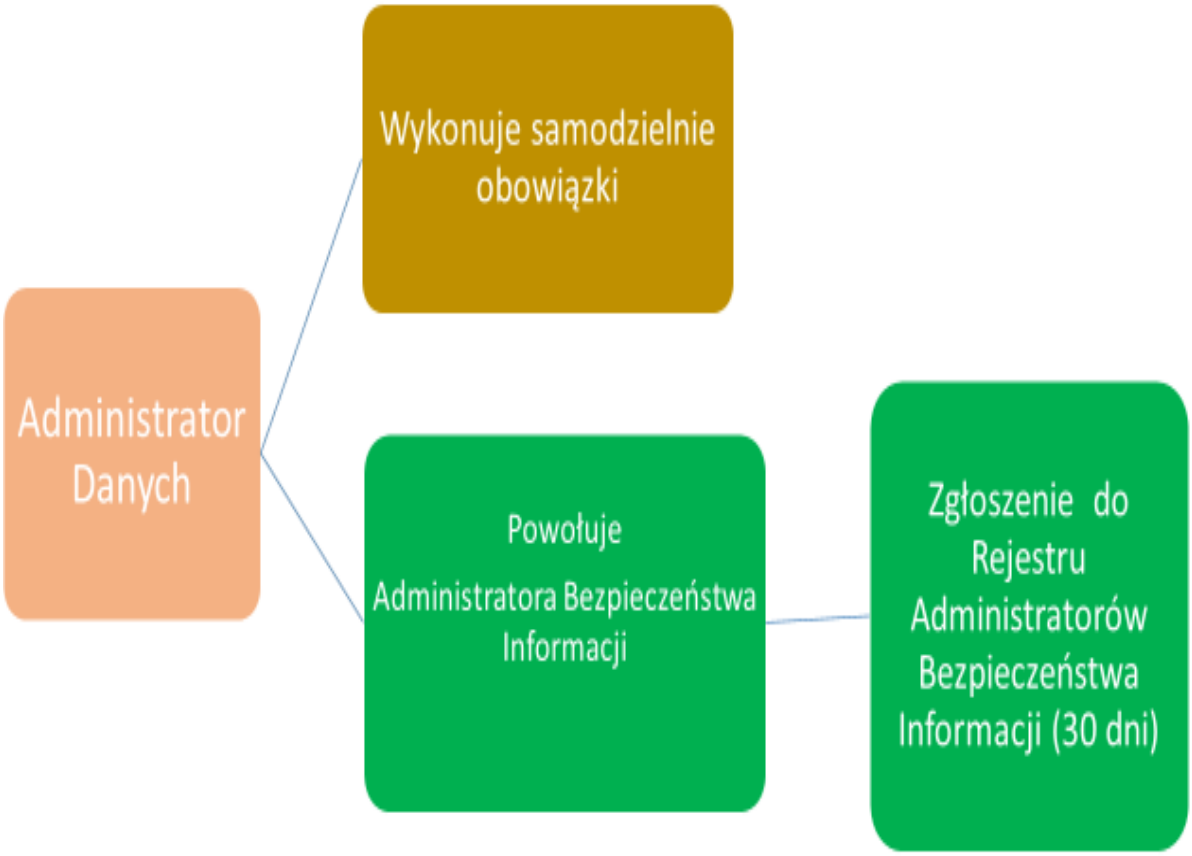

Figure 1. Alternative performance of responsibilities imposed on data controllers
Author's study

Violation of personal data protection

The breach of personal data protection, when there is no appropriate and prompt reaction, may result in a significant economic loss or social damage to the data subject, including the identity-related frauds. Thus, the controller should report to the supervisory authorities about the breach without delay, which is assumed to be within 72 hours. Otherwise, appropriate explanation of the delay should be attached to the report. Individuals, whose personal data could be affected by the breach should be immediately informed so that they can take necessary security measures.

In conclusion, the proposed regulations regarding the important position of the data controller impose on the controller the entire responsibility for processing personal data conducted either by him personally or on his behalf. This regards particularly the documentation, data security, impact assessments, data security officer and the cooperation with a supervising entity. The controller should ensure the compliance of data processing with the regulation to be implemented. This should be verified by independent internal or external auditors.

Bibliography

1. Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
2. European Parliament legislative resolution of 12 March 2014 on the proposal for a resolution of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (general data protection regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
3. Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883,
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
5. STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl
6. Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883, http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
7. Act of 7 November 2014 on facilitation of performance of economic activity (Journal of Laws, 2014, item 1662)
8. European Commission Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm
9. J.Bardadyn Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/
10. Ł. Onysyk Jak prowadzić rejestr zbiorów danych osobowych, http://blog.e-odo.pl/2015/01/13/jak-prowadzic-rejestr-zbiorow-danych-osobowych/
11. P.Janiszewski Projekt rozporządzenia w sprawie realizacji zadań przez ABI http://blog.e-odo.pl/2015/01/05/projekt-rozporzadzenia-w-sprawie-realizacji-zadan-przez-abi/
12. K.Chylińska Nowe rozporządzenie w sprawie abi http://blog.e-odo.pl/author/katarzyna-chylinska/

13. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
14.
15. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/

Abstract

At the beginning of 2015 new regulations regarding the protection of personal data came into force and it is probable that in 2016 the European Union will implement a regulation on personal data protection – a proposal of the European Commission and the European Parliament that will replace the EU Directive 95/46/EC on the protection of personal data. These regulations emphasize the fundamental role of the data controller in ensuring the security of personal data. The data controller is fully liable for the processing of personal data that is conducted either by him or on his behalf. The responsibilities include particularly such issues as documentation, data security, the impact assessment, data security officer and the cooperation with a supervising entity.