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

Conditions and standards regarding medical data processing in new EU regulations

Intoduction

The plan to introduce to EU new regulations regarding the protection of personal data will affect the standards of the current rules of personal data processing, particularly of the data concerning health. The EU resolution has redefined the issue of patients' consent to process their data. It regulates the rules of data storage and deletion, the rules and rights to information, rectification and erasure, the rights to access and obtain information, the right to object and profiling as well as the right to notification about personal data breach. Apart from the discussion on the impact of the above regulations, the article presents the issues related to the planned principles of certification and accreditation of personal data processors as well as the unified rules of personal data flow within and beyond EU borders.

Data subject's consent

Due to the fact that the **consent of the data subject** is the most crucial factor as regards the processing of sensitive data – including the data concerning health – it is important to determine the basic rules regarding the consent.

The consent should be

- given explicitly by any appropriate method enabling a freely given and specific informed indication of the data subject's wishes either by a statement or
- by a clear affirmative action by the data subject, ensuring that the natural persons are aware that they give consent to the processing of personal data.

The clear affirmative action may include ticking an appropriate box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, mere use of a service or inactivity should therefore not constitute consent.

The consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[1]

If the processing is based on the consent, the controller should have the burden of proving that the data subject has given the consent to the processing of their personal data for specified purposes.

If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented clearly distinguishable in its appearance from this other matter.

Irrespectively of other legal grounds for processing, the data subject has the right to withdraw his/her consent at any time. The withdrawal of the consent does not affect the lawfulness of processing based on consent before its withdrawal. The withdrawal of the consent must be as easy as its granting, The controller is obliged to inform the data subject if the withdrawal of the consent may result in the termination of the services or the relationship with the controller.

The consent regards one specific purpose and expires when the purpose ceases to exist or when the processing of personal data is no longer necessary to meet the purpose for which the data were initially collected. The execution of a contract or the provision of a service cannot be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service .

Every natural person whose data are processed should have – as it is provided by the Act on personal data protection - the right to

- access to data which have been collected concerning them, and to exercise this right easily in order to be aware and verify the lawfulness of the process. Consequently every individual should have the following rights:

[1]Amendment 8, Proposal for a regulation , Recital 25 - 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))

- to know and obtain communication in particular for what purposes the data are processed,
- for what period,
- which recipients receive the data,
- what are the general rules of data processing and possible consequences of the processing (at least in the case of profiling).

Moreover, every data subject should have the right to obtain (on demand in an electronic form) the information on personal data being processed and an electronic copy of uncommercial data that are processed in an interoperation format that enables further processing.

This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

Every individual should have the right to rectify his/her personal data and "the right to erasure" the data if the retention of such data does not comply with the Resolution.

Retention of personal data and the right to erasure

The data subject has the right for his/her personal data to be erased and no longer processed

- if the data are no longer necessary in relation to the purposes for which they are collected or otherwise processed,
- if data subjects have withdrawn their consent for processing,
- if they object to the processing of personal data concerning them,
- if the processing of their personal data otherwise does not comply with this Regulation.

However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them. Also, the right to erasure should not apply when the retention of personal data is necessary for the performance of a contract with the data subject, or when there is a legal obligation to retain

this data. As regards the data concerning health, the health service provider retains the medical history for 20 years of the end of calendar year when the last record was made[2].

„The right to erasure*"* in the online environment should also be extended in such a way that a controller who has made the personal data public without legal justification should be obliged to take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation. Thus, in such cases the third parties that process these data should be informed that the processor requested for deleting any links to the data, copies or replications of personal data[3]

However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health and health data processing in relation to health care.

In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled **to object to the processing of any data relating to them**, free of charge and in a manner that can be easily and effectively invoked. *T*he burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

Where the data subject has the right to object to the processing**, the controller should explicitly offer it to the data subject** in an intelligible manner and form, using clear and plain language and should clearly distinguish it from other information [4].

It frequently happens that health care entities apply discs spaces, computing powers or services that provide both disc space, computing power and software, together with a complex management of data retained in the course of processing the data, data concerning health included. The problems occur when due to the termination of the agreement or the dissatisfaction with the services provided, there is a need to change the service provider. Theoretically, the data can be transferred to another similar service provider but, practically, the differences in the data format make the interoperability impossible. Interoperability is a

[2] Article 29, Act of 6 of November 2008 on patients' rights and the commissioner for patients' rights (Journal of Laws of 2009 no.52, item 417

[3] Amendment 27, Proposal for a regulation, Recital 53

[4] Amendment 31,22, Proposal for a regulation , Recital 56, 57 - 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)

property of different entities and IT systems and public registers that the entities apply to work with one another, to share the information and knowledge with the support of business processes and put into practice by the exchange of data with the use of IT systems that the entities have access to.[5]

To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. Data controllers should be encouraged to develop interoperable formats that enable data portability. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. Providers of information society services should not make the transfer of those data mandatory for the provision of their services[6].

Profiling

It is becoming an increasingly more common practice that various financial institutions such as banks, insurance and marketing companies acquire from different sources personal data that were collected lawfully for particular purposes and add them to the other data of their customers, thus developing the so called personality profiles. According to the Resolution 'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyze or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior[7].

Profiling may have two forms. The first one consists in the development of a profile of a particular individual for the purposes of marketing or the preparation of an offer for a customer or in order to assess the customer's capacity to accept particular burdens. The latter one consists in assigning to a set of data additional profiles that are statistically probable, i.e. if an individual has property A, he/she is statistically bound to have features A and C. In other

[5] Article 3 item 18 The Act of 17 February 2005 on the computerization of activities of entities performing public tasks (Journal of Laws of 2005 No.64 item 565)
[6] Amendment 30, Proposal for a regulation , Recital 55
[7] Amendment 98, proposal for a regulation, Article 4, 3a

words to the data that are objective to some extent as they were acquired lawfully or provided by an individual that these data concern, data are added that are statistically probable to accompany them .

The Inspector General for Personal Data Protection (GIODO) indicated that in this way the purpose of data processing is altered and, moreover, a set of personal data is developed that are different from the data provided to the controller by the individual that they concern or from the data the controller is in a justifiable way expected to know [8].

It can be assumed that in such mechanism can be applied in a widely understood health care system; for example, on the basis of enquiries regarding particular medicine or illness, the person will receive adequate advertising of pharmaceuticals or entities that provide appropriate medical services.

As a result of such hazards, it was assumed that profiling, which leads to measures producing legal effects concerning the data subject or similarly significantly affects the interests, rights or freedoms of the concerned data subject, should only be allowed when

- explicitly authorised by law,
- carried out in the course of entering or performance of a contract,
- or when the data subject has given his/her consent.

In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human assessment and that such measure should not concern a child. Such measures should not lead to discrimination against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity. [9]

Every natural person should have the right to object to profiling *w*ithout prejudice to the lawfulness of the data processing,

It should be presumed that profiling based solely on the processing of pseudonymous data does not significantly affect the interests, rights or freedoms of the data subject. When

[8] PROFILOWANIE TO ODRĘBNY CEL PRZETWARZANIA DANYCH OSOBOWYCH, (accessed: 25.05.2011) http://www.giodo.gov.pl/1520098/id_art/4151/j/pl/

[9] Amendment 2, Proposal for a regulation , Recital 58 - 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)

profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous[10].

Restrictions on specific principles and on the rights may be imposed by Union or member state law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, and prosecution of criminal offences or of breaches of ethics for regulated professions, and other specific and well-defined public interests of the Union or of a Member State

The need for system solutions in health care – certification, accreditation

The controller adopts appropriate policies and implements appropriate and demonstrable technical and organizational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with the Regulation, with regard to the latest technological developments, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary[11].

The current legislature lacks provisions as regards the certification of procedures that would ensure the security of data, also in health care entities. As a result, the policies applied may be assessed intuitively, without clearly defined standards that one could refer to.

[10] Amendment 34 , Recital 58 a (new) - Proposal for a regulation , 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 117, Proposal for a regulation , Article 22 - 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)

Consequently, the data subject cannot state in an objective way whether his/her personal data that are being processed in a particular institution, e.g. a health care entity, are secure.

Thus, in order to change the situation

- associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct; such codes of conduct should facilitate the sector to operate in compliance with the regulations[12].
- EU member states should be encouraged to establish certification mechanisms, data protection seals and standardized marks as regards data protection, allowing data subjects a quick, reliable and verifiable assessment of the level of data protection of relevant products and services[13].
    - A 'European Data Protection Seal' should be established on the European level to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing non-European companies to more easily enter European markets by being certified

Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with the Regulation, in particular with the principles regarding personal data processing and policies that ensure the security of processing

It will also be acceptable to accredit specialized auditors to carry out the auditing on behalf of the controller or the processor . Such third party auditors have sufficiently qualified staff, are impartial and free from any conflict of interests regarding their duties. Supervisory authorities grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with the Regulation, the standardized data protection mark named 'European Data Protection Seal'.

The 'European Data Protection Seal' is valid for as long as the data processing operations of the certified controller or processor continue to fully comply with the Regulation. It is presumed that the certification will be valid for maximum 5 years. The

[12] Amendment 51, Proposal for a regulation , Recital 76 - 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)

[13] Amendment 52, Proposal for a regulation , Recital 77 - 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)

European Data Protection Board establishes a public electronic register with all valid and invalid certificates which have been issued in member states

The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with the Regulation.

It is presumed that the Commission is empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms including requirements for accreditation of auditors, conditions for granting and withdrawal, and requirements for recognition and promotion within the Union and in third countries. Such delegated acts confer enforceable rights on data subjects[14].

Transfer of medical data beyond EU borders

In EU a principle is followed that the transfer of personal data within EU is accepted without any additional permissions. A problem emerges when the data are transferred to a country beyond the European Economic Area. With the increasing migration and the plans to abolish the US visa obligation, the problem may be of great significance in the health sector. Individuals who change their permanent address will need a permanent access to the data that are retained in Poland or will need a single transfer of data. Another significant problem is the retention of data in cloud computing servcies as clouds to a large extent belong to American economic entities and, consequently, do not ensure an adequate protection of personal data.

It is a rule that if a third country where personal data are transferred does not ensure on its territory an adequate level of personal data protection, the controller should obtain the consent of a supervisory authority in the form of a decision. The consent is granted under the condition that the controller should ensure adequate safeguards with respect to the protection of privacy and rights and freedoms of the data subject.

The consent is not required if;

- ✓ the data subject has given a written consent;
- ✓ the transfer is necessary for the performance of a contract between the controller and the data subject or taken in response to the data subject's request;

[14] Amendment 135, Proposal for a regulation , Article 38 - 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)

- ✓ the transfer is necessary on important public interest grounds or for the defense of legal claims;
- ✓ the transfer is necessary in order to protect the vital interests of the data subject;
- ✓ the data are generally available.

In the cases other than listed above, the GIODO's consent is not required on the condition that the controller should ensure adequate safeguards with respect to the protection of privacy and rights and freedoms of the data subject by

- standard contractual clauses approved by the European Commission[15] or
- legally binding rules, the so called BCR or policies of personal data protection, approved by the GIODO[16].

According to the Regulation, *binding corporate rules* means personal data protection policies which are adhered to by a controller or processor established on the territory of a member state of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings[17].

The controller has the right of personal data transfer across the EU within a group of undertakings that the controller is a part of when such processing is justified by administrative internal purposes between business groups of undertakings or when an adequate level of data protection as well as the interests of data subjects are secured by internal provisions as regards data protection or equivalent codes of conduct. The approval of the binding corporate rules by a supervisory body means that all controllers belonging to a particular corporation will be able to share the personal data among one another without the GIODO's consent. That is crucial in the case of international bodies that process data within contracts of entrustment. According to the Regulation, the appropriate supervisory authority authorizes in a single document the BCR for a group of undertakings. The rules will enable numerous international transfers of data within Europe and beyond Europe within the group on the condition that they are legally

[15] In line with art. 26 item 4 of the 95/46 /EC directive 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 (O.J.EC L 281 of 23.11.1995, p.31 as amended; O.J.EU – Polish special edition, chapter 13, vol. 15 p.355, as amended)

[16] The solution regarding the binding corporate rules is a sole incorporation to the Polish legal system of the rules applicable after the introduction of BCR for processors set up by Article 29 Data Protection Working Party

[34] Item (17), Amendment 98, Proposal for a regulation , Article 4 - 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)

binding, are applicable to and enforceable by all the members of the group of undertakings of the controller or the processor and their external sub-processors, they apply to their employees, clearly confer enforceable rights to data subjects and are transparent to them.

In cloud computing services, cloud providers often use the external subcontractors to perform a specific task to deliver 24/7 service and maintenance. Therefore, this should be recognized in the Binding Corporate Rules by the supervising authority[18].

Standard contractual clauses[19] that are authorized by the European Commission are contracts between the personal data controller that transfer personal data (data exporter) and the body/bodies that receive them (data importer). Currently, there are two models of Standard Contractual Clauses:

1) appendix to the Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council
2) appendix to the Commission Decision of December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data on third countries (notified under document C(2004) 5271)

A contract includes the information about the personal data exporter and importer and clauses that guarantee an adequate level of personal data protection: i.e. a clause regarding third party, the obligations of data importer and exporter, liability, applicable law, subcontracting of data processing, obligations following the termination of personal data processing. Two appendices are attached to standard contractual clauses:

1) appendix 1, which includes the details concerning the data exporter and importer, data subjects, data categories, processing operations,

[18] Amendment 312, Proposal for a regulation , Article 43.1.a - 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)

[19] As in art.26 item 2 of the 95/46 /EC directive 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

2) appendix 2, which concerns technical and organizational safeguards that are implemented by the data importer[20].

The controller or the processor can transfer personal data to a third country or international organization for historical, statistical or research purposes if:

a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
b) the recipient does not reasonably have access to data enabling the attribution of information to an identified or identifiable data subject; and
c) contractual clauses between the controller or processor and the recipient of the data prohibit re-identification of the data subject and limit processing in accordance with the conditions and safeguards laid down in this article.

A recipient of key-coded data, transferred for scientific research purposes has no means to re-identify subjects, and under this amendment, does not have access to the key and is contractually precluded from re-identifying data subjects. This amendment formalizes a process for reasonably ensuring that key-coded data cannot and will not be re-identified by recipients located in third countries, allowing for the transfer of such data without further burdens.

[20] STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl http://www.e-ochronadanych.pl/przekazywanie_danych_osobowych_do_panstwa_trzeciego.php?news_id=2455

Bibliography

1. Act of 6 of November 2008 on patients' rights and the commissioner for patients' rights (Journal of Laws of 2009 no.52, item 417
2. 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)
3. European Parliament legislative resolution of 12 March 2014 on the proposal for a directive 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)
4. Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883,
5. 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
6. STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl
7. Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883, EU website http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
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. PROFILOWANIE TO ODRĘBNY CEL PRZETWARZANIA DANYCH OSOBOWYCH, (accessed: 25.05.2011) http://www.giodo.gov.pl/1520098/id_art/4151/j/pl/
11. M. Chmielecki UNIJNA REFORMA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH - INFORMACJE OGÓLNE e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
12. M. Cwener PROPOZYCJE ZMIAN W ZAKRESIE PRZEPISÓW DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH – CZ. I; ii OGÓLNE e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
13. K. Szymielewicz Półprzepuszczalny standard ochrony danych https://panoptykon.org/wiadomosc/polprzepuszczalny-standard-ochrony-danych
14. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
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

The plan to introduce to EU the new regulations regarding personal data protection will have an impact on the standards of the current principles of personal data protection, particularly of the data concerning health. The EU resolution has redefined the issue of patients' consent to process their data. It regulates the principles of data storage and erasure, the rules and rights to information, rectification and erasure, the rights to access and obtain information, the right to object and profiling as well as the right to notification about personal data breach. Apart from the discussion on the impact of the above regulations, the article presents the issues related to the planned principles of certification and accreditation of personal data processors as well as the unified rules of personal data flow within and beyond EU borders.