Available online at www.worldscientificnews.com

World Scientific News

WSN 85 (2017) 19-27 EISSN 2392-2192

States of emergency – selected problems regarding the personal data protection

Tomasz Soczyński

Faculty of Law and Administration, University of Gdansk
6 Jana Bażyńskiego Str., 80-309, Gdańsk, Poland

E-mail address: tomek_soczynski@yahoo.com

ABSTRACT

The following elaboration has been produced following the analysis of the problem regarding the protection of privacy and private life as well as the personal data themselves under the circumstances of life-threatening situations or the state of emergency. The solutions stipulated by the domestic and EU legislation have been analysed with emphasis put over accessing processes to personal data , both indispensible and proportional ones, carried out with an intention to secure public safety, including the protection of human life especially as a reaction to natural disasters or catastrophes caused by humans, protection of other important objectives that lie within general public interest, for instance when data processing remains necessary for humanitarian purposes, including the monitoring of epidemics and their dispersion. Personal data are characterised by various degrees of sensitivity and criticality. Some of them may require an additional level of protection and special treatment. GDPR makes it possible for the Member States to clarify their provisions, including such ones regarding the processing of personal data of special categories (also referred to as sensitive data), they do not exclude an option to specify in the legislation of a Member State the circumstances of precise situations related to data processing, including the precise clarification of conditions which decide whether data processing remains compliant to the law. Personal data processing under extraordinary circumstances may imply, as an exception, the necessity to transfer the data if such action is required by important public interest set forth by the EU legislation or the relevant provisions of a Member State or if such transferring occurs from the register established by law and intended to provide an insight for the general public or persons maintaining legally valid interest, for instance public health units in order to establish infectious contacts in case of infectious diseases outbreak. A subsequent part of the article focuses on the issues related to the course of actions under state of emergency, i.e. it presents the proceedings to be carried out in emergency state and specifies the concerns on emergency call processing, including the personal data.

***Keywords*:** data protection, general data protection regulation, information security

1. INTRODUCTION

Dynamics of modern technologies has led to civilisation changes that cannot be boiled down to ameliorations in the communications processes, acquisition and processing of data, all of which influences the formulation of the so called information society.

Information (in Latin *informatio* – notification about something, communicating something; notification, instruction) lied foundations to the theory of information that encompasses coding, transforming, transferring and storage of information as well as limiting the factors that disturb it.

In colloquial language the following notions are used interchangeably: information, data, personal data, sensitive data, etc. The adopt the meanings depending on a linguistic and situational contexts. The notion of data has not much to do with a primary Latin term datum (the term, i.e. calendar notification of a day, a month, a year). In humanities the word data means the features or properties. In sciences, i.e. IT, data mean a collection of numbers and texts in various forms (e.g. signs, speech, diagrams, signals).

TOGA metatheory according to Gadomski[1] defines data as everything that is or can be processed by mind or by a computer while information means the data referring to a given area of human activity or that of artificial intelligence. In line with that definition, information constitutes the data while not all data constitute information. The numbers themselves are always the data, however they become information when related to a given area. The numbers 134 and 9612XXX6822 are examples of data. Determination of a car accident venue at the 134th kilometre of an A-4 motorway remains a piece of information. PESEL (statistical) number 9612XXX6822 is a personal detail, i.e. a special type of information.

Implications and conditioning of the technological revolution require to take actions intended to make order in the sphere regarding information processing and protection, which is related to the introduction of the relevant regulations. Pursuant to article 47 of the Polish Constitution every person has the right to protect their private and family life, to be honoured and protect their good name as well as to decide about their private lives. Article 51 clause 1 and 2 of the Constitution specifies that none can be committed to reveal any information referring to themselves unless ordered to do so by a relevant act.

Public authorities cannot acquire, collect and share information on the citizens except for such ones that remain indispensable in a democratic country, which is rightfully specified by the authors of "Information protection in the states of emergency" *(Ochrona informacji w stanach zagrożeń)* [2].

---

[1] A.M. Gadomski, Information, Preferences and Knowledge. http://erg4146.casaccia.enea.it/wwwerg26701/gad-dict.htm

[2] Ochrona informacji w stanach zagrożeń st. bryg. dr inż. Bogdan Kosowski st. kpt. mgr inż. Robert Piec, Szkoła Główna Służby Pożarniczej, Warszawa.
https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwil9ozH1ZfTAhVEbRQKHRrQADQQFggxMAI&url=http%3A%2F%2Fwww.uwm.edu.pl%2Fmkzk%2Fupload%2Freferaty%2F41_ochrona_informacji_w_stanach_zagrozen.doc&usg=AFQjCNEKjj33nV4UwDHRMKrbkssU50Z_8Q&sig2=tTKtZ4ghBRo7X4UuvZXa7w&bvm=bv.152174688,d.d24&cad=rja

Another important, yet new, element of data processing protection remains the provisions of Resolution of European Parliament and Council 2016/679 dated 27th April 2016 on physical persons protection in personal data processing and the free flow of such data as well as lifting the directive 95/46/WE (GDPR)[3]. The aforementioned resolution shall replace the provisions of the Act dated 29th August 1997 on personal data protection (i.e. the Journal of Laws from the year 2016, item 922) (UODO)[4] together with secondary legislation to the said act. The provisions shall come into force on 25th May 2018 therefore it is justified to commence the relevant processes during the transition period to get adjusted to the new regulations. In order to define the changes stipulated by the new regulation better, the current and future legal requirements have been analysed.

2. PERSONAL DATA

Legal provisions define two types of personal data. The y contain ordinary data and specially protected data (also referred to as sensitive data). While comparing the definitions contained in the currently binding Personal Data Protection Act (UODO) we cannot forget to refer to the definition of personal data. In line with UODO, ordinary personal data include all information regarding an identified physical person or the one to be identified. An identifiable person is anyone whose identity may be established directly or indirectly, especially by referring to their ID number or by one or several specific factors determining their physical, physiological, mental, economic, cultural or social features.

Special attention is required to the fact that the legislator has failed to close the catalogue of information which must be regarded as personal data subject to protection, i.e. information such as a telephone number, a computer IP address, email address, cookie files, IMEI number of a mobile phone, nick. Login may constitute a personal datum as well.

The term sensitive data is commonly applied to the data that receive special protection- article 27 of the Act dated 29th August 1997 on personal data protection: data revealing racial and ethnic background, political beliefs, religious or philosophical views, religious background, political party or trade union membership, data on addictions or sexual life, convictions, sentences, fines and tickets, state of health, genetic codes. It must be noted that pursuant to article 29 of the Opinion from the EC Working Group specifies that personal data should also include biometric data projections and DNA, which may be used to establish the identities of people.

It must be noted however that article 4 of GDPR presents the new catalogue of definitions. GDPR makes it possible for the Member States to clarify their provisions, including such ones referring to processing of various personal data categories (hereinafter referred to as sensitive data). The following enactment does not exclude an option to specify in the legislation of a Member State the circumstances of precise situations related to data

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 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) http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

[4] USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883

processing, including the precise clarification of conditions which decide whether data processing remains compliant to the law.

3. PERSONAL DATA PROCESSING UNDER STATE OF EMERGENCY

Polish Constitution dated 2nd April 1997 specifies three extraordinary states:

- Martial law,
- State of emergency,
- State of natural disaster.

In line with article 228 clause 2 of *the Polish Constitution* extraordinary state may be introduces by means of an act or an enactment which are subject to being made public. The introduction of the extraordinary state influences the principles of functioning for public authorities, the range of liberties applicable and the rights of an individual. Such questions remain independent of the organs and have been specified in the Constitution and the act regarding individual types of extraordinary states. Consequences of the extraordinary state introduction have not been left for the discretion of the authorities but have been regulated by the relevant act, i.e. article 17 clause 1 of the Act dated 18th April 2002 on the state of natural disaster (Journal of Laws number 62, item 558, as amended).

The following services participate in the prevention against natural disasters and in the removal of their consequences: State Fire Brigade and other units of fire protection, Police, Boarder Guard, SAR services, healthcare entities, especially State Emergency Medical Services and other state offices, agencies, inspections, guards and services.

In line with the preamble to 73 of GDPR, EU legislation or the legislation of a Member State may anticipate the constraints regarding: certain principles and the right for information, accessing the personal data, their rectification or removing, the right to transfer the data, the right to object, decision based on profiling, notification of a person whom the data refer to, infringements on the personal data protection as well as defined duties of controllers, unless it is indispensable and proportional within a democratic society to provide public safety, including the protection of human life.

The aforementioned includes especially reacting to natural disasters and catastrophes brought about by humans, counteracting to crime, running the preparatory proceedings, prosecution of forbidden acts or enforcement of penalties, including the protection against threats to public safety and prevention from such ones, or prevention against the infringements on ethical principles in the case of regulated professions, protection of other important objectives lying within the general interest of EU or a Member State, especially economic or financial interests of UE or a member State bearing a special importance, running the public registers due to the general public interest, further processing of archived personal data in order to provide precise information on political beliefs within former political systems of totalitarian states or provide protection with regards to a person whom the data refer to or rights and liberties of other individuals, including the objectives in the field of social protection, public healthcare and humanitarian aims.

Such constraints should remain compliant with the requirements set forth by the Charter of Fundamental Rights and the European Convention on human rights protection and basic

liberties[5]. An option must be anticipated that will allow to transfer the data if important public interest specified by EU legislation or the legislation of a member State so requires or if such a data transfer occurs from the register formulated based on the law and with an intention of providing an insight into it for the general public or persons having a justified interest in doing so.

Such exceptions should be applicable to transferring the data which is required and even remains indispensable due to important public interest, for instance during international data exchange between organs on competition, taxation or customs authorities, organs of financial supervision, services responsible for social assistance or public healthcare in order, for example, to establish the infectious contacts during epidemics or eliminate doping in sports. Transferring the personal data should be regarded as lawful also under the circumstances necessitating to safeguard the interests bearing a special importance for the vested interests of the person whom the data refer to or any other person, including physical integrity or life and the person whom the data refer to is unable to grant their consent.

Article 7d of the Directive 95/46/EC[6], stating that data processing remains indispensable to safeguard the vested interests of the person whom the data refer to, could be relevant in some instances of "applications related to safety"[7], such as: preventing the catastrophes, fire brigade inspection, rescuing the victims of snow-related and mountain accidents, etc. However, bearing in mind that article 7 letter d) must be interpreted in a strict manner, taking such applications into consideration pursuant to article 7 letter c), article 7 letter e) or article 7 letter f) might constitute a better approach[8].

In case when the protection level is found insufficient, the EU legislation or the legislation of a Member State may, due to an important public interest, impose constraints over the transfer of certain categories of data to third countries or international organisations. Member States ought to advise the European Commission on such provisions.

Each personal data transfer with regards to the person whom the said data refer to and who is physically or legally unable to grant their consent to an international humanitarian organisation in order for such the organisation to execute the tasks imposed over it by the Geneva Convention or to meet the requirements of international humanitarian law applicable in war conflicts may be considered as indispensable due to an important public interest or included into the vested interests of the person whom the data refer to.

[5] Gonzales Fuster G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014;

[6] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[7] Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

[8] See the WP 29 analysis concerning the eCall system: Working document on data protection and privacy implications in eCall initiative of 26th September 2006 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf

4. COURSE OF ACTION IN A CRITICAL SITUATION

Table 1. Proceedings in a critical situation.

Threat evaluation	Natural disaster – natural catastrophe or technical failure which consequences pose the threat to the lives and health of a big group of people , property of large size or the environment over a vast area and assistance and protection may be commenced only by application of extraordinary means
Information	Information Safety Controller or any person authorised by them must be notified on the threat, its scale and the remedies taken. Telephone numbers to the Information Safety Controller and any persons to be contacted in case of a natural disaster must be known to the labour force.
Rescue operation	Persons participating in the rescue operation are eligible to enter the premises in which personal data are processed without any authorisation required by law. In case of evacuation, the users staying in the premises where personal data are processed remain committed to stop their work and safeguard the personal data, if possible, prior to leaving the premises.
Safeguarding the persona data	Once the rescue operation has terminated, the Information Safety Controller and the users present should, if possible, safeguard the personal data against unauthorised accessing.

5. PROCESSING OF ALARM CALLS, INCLUDING THE PERSONAL DATA

In line with article 11 of the *Act dated 22nd November 2013 on the emergency notification system* the minister relevant for public administration remains the data controller pursuant to the act on protecting the personal data stored in the system. The said minister may authorise the head of a province or an entity, specified by article 7 clause 2 of the aforementioned act, to grant or withdraw, on his behalf, any authorisations to process the personal data stored in the system for ay persona involved in personal data processing. The head of a province or an entity, specified by article 7 clause 2 of the aforementioned act, creates and updates the register of persons authorised to process the personal data within the system. With regards to the data processed within the system, the duty to provide information set forth by article 24 clause 1 of the personal data protection act does not apply.

While considering the provisions of the Act dated 22nd November 2013 on the emergency notification system, one must pay special attention to the fact that in line with article 14 h clause 2 the Commander of the Fire Brigade remains the controller of the data processed in SWD PSP, as stipulated by the Personal Data Protection Act (UODO) dated 29th August 1997 (Journal of Laws from the year 2015, item 2135 and 2281). Simultaneously, in line with article 21 g clause 2 , the Commander of Police Forces remains the controller of the

data processed by Police SWD , pursuant to the act dated 29 August 1997 The Personal Data Protection Act (UODO).

As the above mentioned provisions reveal, the legislator has applied the construction of the personal data co-controllers. The collection of data within SDW of the Police or of the Fire Brigade remains an integral part of the emergency notification system with regards to a two-way data share. Legal construction of this kind had been assumed to start from 1st April 2016 and constitutes a quasi institution for data co-controlling. In line with article 23 clause 2a of the Personal Data Protection Act public entities are regarded as one data controller if data processing serves for the same public interest. Pursuant to GDPR the co-controllers (at least two of them) jointly establish the goals and manners to process the data as well as the mutual relations between them. Predominantly, they ought to set forth the ranges of their responsibilities in order to meet the requirements resulting from new regulations.

On a par with article 11 of the *Act dated 22nd November 2013 on emergency notification system*, the Commander of the Fire Brigade may authorise the heads of organisational units to grant or withdraw , on his behalf, the authorisations for personal data processing within the Fire Brigade SWD to any persons involved in the processing of such data. He also creates and updates the register of the persons authorised to process the personal data stored in the Fire Brigade SWD.

Establishing the legal basis and the purpose for data transferring to the entities remains one of the key aspects for personal data processing safety in case of emergency calls. It must be noted here that the purpose related to life saving is different from the Police investigation. The provisions of article 10.4 of the Act on emergency notification system stipulates that the head of a province or an entity specified by article 7 clause 2 shall process the data registered within the IT system, including the recording of the telephone calls, personal details of a notifying person, details regarding any other persons mentioned during the call taken up, geographical positioning, contact details or incident descriptions and shall make them available when having been applied for it by the court, prosecutor's office or Police.

The situation when the recorded call is made public has been described by the PANOPTYKON foundation in the article entitled "A bit of confidentiality in a critical situation" *(Odrobina poufności w kryzysowej sytuacji)*[9]. The General Inspector for Personal Data Protection has applied to the Poviat Commander of Police in Żary[10] paying attention to the fact that publication of the recordings containing the personal details of people contacting the Police remains unacceptable. Making such a recording public infringes on the personal data protection act. The only prerequisite that would legitimise the actions of this kind could be the consents granted by the persons whom the data refer to. When the said consent cannot be obtained the material recorded must be modified to make the identification of the calling persons as well as other persons mentioned impossible.

Under the circumstances other than natural disasters, emergency calls and the aforementioned extraordinary situations, all generally valid principles related to personal data must be applied.

[9] Odrobina poufności w kryzysowej sytuacji https://panoptykon.org/wiadomosc/odrobina-poufnosci-w-kryzysowej-sytuacji

[10] Wystąpienie Generalnego Inspektora Danych Osobowych do Komendanta Powiatowego Policji w Żarach https://panoptykon.org/sites/panoptykon.org/files/stanowiska/wyst.giodo_kpp-zary.pdf

6. CONCLUSIONS

In line with article 7 of the Polish Constitution the organs of public authorities shall act based on and within the law. Acting on the basis of and within the law means an action which is based on the wording of a given provision. While processing the personal data pursuant to the binding Personal Data Protection Act we remain committed to apply the proper principles regarding their processing, being stipulated especially by article 23 clause 1 (for ordinary data) and article 27 clause 2 (for sensitive data), i.e.:

- Legal compliance principle
- Purpose limitation principle
- Principle of adequacy and correctness
- Principle of necessity

Pursuant to article 5 of GDPR the following principles must be added:

- Integrity and confidentiality
- Accountability

While fulfilling an obligation to include data protection by design and by default, a personal data controller remains committed to act in line with the legislation and the current state of the art at all times. They are under obligation to provide technical and organisational safety for personal data protection, especially when granting another entity with personal data processing.

References

[1] Siemieniak P. (2016). The Impact of the Sentence C-362/14 in the Case Maximillian Schrems Against Data Protection Commissioner Over the Personal Data Transfer from the European Union to the United States of America. *World Scientific News* 51, 57-61.

[2] Agre, P.E., Rotenberg, M. (1997). Technology and Privacy: The New Landscape, MIT Press.

[3] Moore, A. (1998). Intangible Property: Privacy, Power, and Information Control. *American Philosophical Quarterly*, Vol. 35.

[4] Singleton, S. (2000). Privacy and Human Rights: Comparing the United States to Europe in CEI Staff (ed.), The Future of Financial Privacy, Washington DC, Competitive Enterprise Institute.

[5] Solove, D. J. (2004). The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure. *Duke Law Journal*. Vol. 53, 967-1062.

[6] Bennett C., Raab Ch. D. (2003). The Governance of Privacy: Policy Instruments in Global Perspective, Ashgate.

[7] Azevedo Cunha M. V. (2013). Market integration trough data protection. An Analysis of the Insurance and Financial Industries in the EU. Springer

[8] Flaherty D. H. (1992). Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, The University of North Carolina Press.

[9] Gonzales Fuster G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer.

[10] Greenleaf G. (2012). The influence of European data privacy standards outside Europe: Implications for globalisation of Convention. *International Data Privacy Law*, Vol. 2, Issue 2, 1, 68-92.

[11] Shaffer G. (2000). Globalization and social protection: the impact of EU and international rules in the ratcheting up of U.S. data privacy standards. *Yale Journal of International Law*, Vol. 25, 10-21.

(Received 12 August 2017; accepted 30 August 2017)