

DOI 10.5817/MUJLT2018-2-4

QUO VADIS OPEN DATA?

by

JOZEF ANDRAŠKO*, MATÚŠ MESARČÍK**

New technologies have irreversibly changed the nature of the traditional way of exercising the right to free access to information. In the current information society, the information available to public authorities is not just a tool for controlling the public administration and increasing its transparency. Information has become an asset that individuals and legal entities also seek to use for business purposes. PSI particularly in form of open data create new opportunities for developing and improving the performance of public administration.

In that regard, authors analyze the term open data and its legal framework from the perspective of European Union law, Slovak legal order and Czech legal order. Furthermore, authors focus is on the relation between open data regime, public sector information re-use regime and free access to information regime.

New data protection regime represented by General Data Protection Regulation poses several challenges when it comes to processing of public sector information in form of open data. The article highlights the most important challenges of new regime being compliance with purpose specification, selection of legal ground and other important issues.

KEY WORDS

Data Protection, GDPR, Open Data, PSI Directive, Public Sector Information

* jozef.andrasco@flaw.uniba.sk, JUDr. Jozef Andraško, PhD. is an assistant professor at Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava, Slovakia.

** matus.mesarcik@flaw.uniba.sk, Mgr. Matúš Mesarčík, LL.M. is an internal PhD. candidate at the Department of Administrative and Environmental Law and Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava, Slovakia.

1. INTRODUCTION

Public administration faces several challenges in the context of modernization and development of new technologies. Increasing transparency and participation of citizens in public affairs is a legitimate question and issue for many (especially) post-communist countries. Publication of information related to public administration is a strong tool to develop aforementioned issues connected to transparency. Re-use of public sector information and open data are concepts that oscillate in the current discussions.

The first part of the article is devoted to the analysis of public sector information and open data. The emphasis is put on differences and similarities between notions and selected issues. The assessment is conducted in the light of legal orders of Slovak Republic and Czech Republic including the evaluation of related legislation of the European Union.

The second part of the article focuses on processing of open data in the context of data protection. General Data Protection Regulation and national data protection laws “after GDPR” significantly challenge simple facilitation of using previously published personal data. Issues of purpose and legal ground for processing are of the primary interest. The emphasis is put on the legislation and soft law of the European Union and short remarks are made towards related data protection issues in Slovak Republic and Czech Republic.

2. PUBLIC SECTOR INFORMATION AND OPEN DATA – TODAY AND TOMORROW

2.1 OPEN DATA¹

The open data regime is based on the assumption that public administration authorities produce, collect and process a large amount of public data in different areas like transport, culture, finance, science and research, the environment or various statistics. In the context of the release of open

¹ The term open data is neither defined by generally binding legal act in the Slovak legal order, nor are there defined relations between the term information and data. These two terms are often understood to be synonymous what is not true. Olejár claims that information is the content of the data, and the data is only a form of record of information. In other words, the same information can be recorded in different forms, e.g. information 10 can be recorded as ten, zehn, X. See Olejár, D. et al. (2015) *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, p. 5. More on the issue of difference between data and information see Polčák, R. (2016) *Informace a data v právu. Revue pro právo a technologie* 7, pp. 67–91.

data, it should be borne in mind that public administration has an important position. First of all, public administration creates a large amount of information within fulfilling its tasks. Secondly, a large amount of this information is public and should, therefore, be made available for re-use. Despite the fact that public administration has a large amount of information, it publishes them in a limited amount or in an inappropriate format. Such information can be considered as public data but not open data that can be processed by machine in an automatic way.

By opening public administration data² for commercial or non-commercial purposes in the form of different application development, the economic potential of public administration data can be fully exploited.³ Despite the undeniable economic potential of public administration data, it should be noted that the main purpose of the open data regime is to ensure transparency in public administration and to increase public interest in public administration.⁴

The importance of public administration open data also lies in the fact that experts (researchers, scientists, journalists, web developers, mobile or other software applications) can use the open data repeatedly and create new commercial or non-commercial services that can serve the public.

In accordance with the definition of the Open Knowledge Foundation, open data may be defined as information which is published on the Internet in a way that does not impose any technical or legal obstacles in its use. All users are authorized to further dissemination of this information under the condition that they will indicate the author of the information in question, as well as, other users have the same rights to handle distributed information.⁵

The non-profit organization Sunlight Foundation has defined 10 principles for opening up government information. These principles provide a lens to evaluate the extent to which government data is open and accessible to the public. The principles are completeness, primacy,

² Term public administration data is a synonym of the term government data.

³ The estimated market value of open public administration data in the EU is € 55.3 billion for 2016, up to 325 billion by 2025 what is representing about 25,000 new jobs in the field of open data. [online] Available from: <http://www.europeandataportal.eu/en/content/creating-value-through-open-data> [Accessed 1 March 2018].

⁴ For more information about transparency in the context of free access to information see: Munk, R. (2017) *Attempt to increase the transparency*. Bratislava law review, Vol. 1, No. 2, pp. 167–173.

⁵ *Open Knowledge Foundation: The Open Data Manual* (2011). [online] Available from: <http://opendatahandbook.org/> [Accessed 1 March 2018].

timeliness, ease of physical and electronic access, machine readability, non-discrimination, use of commonly owned standards, licensing, permanence and usage costs.⁶

2.2 TYPES OF OPEN DATA USED IN PUBLIC ADMINISTRATION

International initiatives such as the Open Data Charter⁷, signed on 18 June 2013 by G8 leaders and the Open Government Partnership, place emphasis on making public administration information available to strategic datasets that represent a valuable asset for society as a whole.

Based on the abovementioned international initiatives and on the preferences expressed in the open consultation, *Guidelines on recommended standard licenses, datasets and charging for the reuse of documents 2014/C 240/01* defined that users who want to re-use public administration data require the following five thematic dataset categories:

Category	Examples of Datasets
1. Geospatial data	Postcodes, national and local maps (cadastral, topographic, marine, administrative boundaries, etc.)
2. Earth Observation and Environment	Space and <i>in situ</i> data (monitoring of weather, land and water quality, energy consumption, emission levels, etc.)
3. Transport Data	Public transport timetables (all modes of transport) at national, regional and local levels, road works, traffic information, etc.
4. Statistics	National, regional and local statistical data with main demographic and economic indicators (GDP, age, health, unemployment, income, education, etc.)
5. Companies	Company and business registers (lists of registered companies, ownership and management data, registration identifiers, balance sheets, etc.)

Table 1: Dataset categories

Other categories may be considered as core or high-value data, depending on circumstances like importance for strategic objectives, market developments, social trends, etc. It is also recommended that the responsible public authorities assess which dataset should be released as a priority.

⁶ Exhaustive description of principles. [online] Available from: <https://sunlightfoundation.com/policy/documents/ten-open-data-principles/> [Accessed 1 March 2018].

⁷ Available from: <http://opendatacharter.net/history/#> [Accessed 1 March 2018].

2.3 OPEN DATA IN PRACTICE

The best-known example of the use of public administration data in the Slovak Republic is the open-ended project, created by the Fair-Play Alliance and Transparency International Slovakia. The project was initiated when the compulsory publication of all contracts relating to the public funds and state or self-government property was applied in 2011. The main role of the open contracts website is to help citizens to read, search and evaluate the advantageousness of contracts concluded by state and state institutions.⁸

Open government data can also be used to analyze voting in Parliament. One of the examples is the Czech project *KohoVolit.eu*, through which citizens can monitor the work of members of Parliament, their attendance and voting. Users of this app may even contact parliamentarians.⁹

Transport data comprise an important source of public administration open data. After London traffic data was released, more than 500 applications were made available to enable the public to obtain up-to-date information on the use of individual lines to optimize the operation of urban public transport.¹⁰ The availability of information by the British Ministry of Transport allows searching for current restrictions on the roads, such as work on motorways, detours or motorway closures. This information helps drivers make travel time more efficient.¹¹

Another example is the use of crime data from Santa Cruz, California, where local police began to record crime data in detail. With the analysis of collected data, the police have been able to predict at what street is in a certain time a high risk of committing various crimes, such as car theft or burglary.¹² The release of the data on criminality also affected the real estate market. Buyers began to buy real estate according to the security of the specific area.

In 2005, the Guardian daily requested data on the success of 400,000 cardiology operations over the last 5 years. Journalists analyzed cardiology

⁸ Otvorené zmluvy. [online] Available from: <http://otvorenezmluvy.sk> [Accessed 20 September 2018].

⁹ KohoVolit.eu. [online] Available from: <http://kohovolit.eu> [Accessed 20 September 2018].

¹⁰ London datastore. [online] Available from: <http://data.london.gov.uk/> [Accessed 20 September 2018].

¹¹ Live map of London Underground. [online] Available from: <http://traintimes.org.uk/map/tbe/> [Accessed 20 September 2018].

¹² Crimereports.com. [online] Available from: <https://www.crimereports.com/agency/santa-cruzspd> [Accessed 20 September 2018].

information and published the results of the analysis. As a result of this activity, people began to select hospitals with statistically the highest success rate for their operations, which had an impact on citizens' lives. The mortality fell by 21% or by one-third in specific types of surgery, even though the number of patients has risen.¹³

The most classic example of the use of open data is data on legislation. In the UK, all laws, legal regulations, and legislation changes since 1267 can be found in one place.¹⁴ In the context of the publication of legislation in the Slovak Republic, the portal *Slov-Lex* operated by the Ministry of Justice of the Slovak Republic can be mentioned.¹⁵

The issue of open data plays a major role at European Union (hereinafter referred to as the "EU") level. The EU Open Data Portal (hereinafter referred to as the "Portal") has been created as a single point of access to the data of the institutions as well as other EU bodies. These data are freely available for re-use, both for non-commercial and commercial purposes. The Portal aims at utilizing the economic potential of information as well as to increase transparency and accountability of institutions and other bodies in the EU.¹⁶

2.4 EU APPROACH TO OPEN DATA

Discussions on information collected, produced and disseminated by public authorities within their competences extend to the 1970s and 1980s. With the advent of the Internet, information began to be considered as assets of economic value. Efforts to adopt legislation on the re-use of information created by public authorities have been completed by the adoption of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (hereinafter referred to as the "PSI Directive").¹⁷

The PSI Directive was amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending

¹³ Boseley, S., UK heart operation death rates fall after data published. *The Guardian*. [online] Available from: <https://www.theguardian.com/lifeandstyle/2009/jul/30/heart-surgery-death-rates-fall> [Accessed 20 September 2018].

¹⁴ Legislation.gov.uk. [online] Available from: <http://www.legislation.gov.uk/> [Accessed 20 September 2018].

¹⁵ Slov-lex.sk. [online] Available from: <https://www.slov-lex.sk/domov> [Accessed 20 September 2018].

¹⁶ Datasets from: Data.europa.eu. [online] Available from: <https://data.europa.eu/euodp/en/data> [Accessed 20 September 2018].

Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance (hereinafter referred to as the “PSI Directive 2013”) in 2013.¹⁸

We use terms PSI Directive and PSI Directive 2013 in the text of this article. When using the term PSI Directive 2013 in the text of this article, we point out the new legislation. If we use the term PSI Directive we refer to its consolidated version.

The PSI directive focuses on the economic aspects of re-use of information rather than on the access of citizens to information. It encourages the EU Member States to make as much information available for re-use as possible. The directive in question provides a common legal framework for a European market for government-held data.¹⁹

The term public sector information (hereinafter referred to as the “PSI”) is not directly defined in the PSI Directive. Therefore, terms such as a document, a public sector body and finally the term re-use will help us to clarify the term in question.

Document means any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) as well as any part of such content.²⁰

The PSI Directive defines public sector body as

“state, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law.”²¹

¹⁷ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. *Official Journal of the European Union* (2003/L345/90). 31 December. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32003L0098> [Accessed 3 March 2018]. More on the issue of PSI Directive and its transposition into particular EU Member States legal orders see Janssen, K. (2011). The influence of the PSI directive on open government data: an overview of recent developments. *Government. Information Quarterly*, 28, pp. 446–456.

¹⁸ Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance. *Official Journal of the European Union* (2013/L1751/1) 27 June. Available from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013L0037> [Accessed 3 March 2018].

¹⁹ The European Commission proposed a new PSI Directive on 25 April 2018. Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast) COM/2018/234 final – 2018/0111 (COD). 25 April 2018. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information> [Accessed 11 September 2018].

²⁰ PSI Directive, Article 2 (3).

²¹ *Ibid.*, Article 2 (2) (c).

Body governed by public law is defined as any body:

“a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

b) having legal personality; and

c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law.”²²

European legislature defined the term re-use as the

“use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced.”²³

In other words, public sector documents are information that a public sector body handles and there is a demand for further processing and use outside the public sector. This process is called re-use of public sector information.

The PSI Directive 2013 has brought a significant shift in the obligation for the EU Member States to make all documents available for re-use unless they are restricted or excluded by national rules and are not subject to other exceptions stated in the PSI Directive. Prior to the adoption of the PSI Directive 2013, EU Member States had the option, not the obligation to make documents available.

In that regard, the PSI Directive applies only to documents that may be made publicly available on the basis of the rules laid down in the legislation of the EU Member States. In this case, it is possible to talk about a general approach to documents. On the other hand, if citizens or businesses have to prove a particular interest in obtaining access to documents, we talk about the privileged approach when access to documents is restricted.

²² Ibid., Article 2 (2) (c).

²³ Ibid., Article 2 (4).

It is necessary to point out that PSI Directive does not contain provisions on access to information which is the basic precondition for their re-use. The European legislator has left access to information on the legislation of the EU Member States. This may be justified, in particular by the limited legislative powers of the EU in regulating the right of access to information. It is not the intention of the authors to focus on the issue of access to information.

Consequently, in the light of the foregoing considerations, it could be said that the EU legal framework regarding re-use of information held by the public administration is focusing more on PSI rather than on open data. It is necessary to point out that open data can be considered as information that is freely available on the Internet in a structured and machine-readable format and accessible in a manner which does not impose any technical or legal obstacles in its use.²⁴

2.5 OPEN DATA IN THE SLOVAK LEGAL ORDER

The issue of open data is partially regulated by *Act No. 211/2000 Coll., On Free Access to Information and on changes and amendments to certain acts* (hereinafter referred to as the “Freedom of Information Act”). In the case of Slovak legal order, the issue of open data is connected with the PSI re-use regime that is regulated by the Freedom of Information Act.²⁵

Act No. 340/2015 Coll., amending the Freedom of Information Act created more favorable legal conditions for the re-use of information created by public authorities.²⁶ In particular, the disclosure of information in electronic form is preferred and where possible and appropriate, as open

²⁴ More on the issue of open data concept see Verhulst, S., & Young, A. (2016). *Open Data impact, when demand and supply meet. Key finding of the open data Impact case studies*. Opgehaald van. thegovlab.org. [online] Available from: <http://odimpact.org/key-findings.html>; Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32 (4), pp. 399–418; Dawes, S., & Helbig, N. (2010). Information strategies for open government: Challenges and prospects for deriving public value from government transparency. *Electronic Government*, 6228, pp. 50–60; Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 29, pp. 258–268; Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European Journal of ePractice*, pp. 1–13.

²⁵ Specific provisions on the re-use of information were transposed into Slovak legal order by Act No. 341/2012 Coll., amending the Freedom of Information Act (with effect from 1 December 2012). By adopting the act in question, a new independent regime of the right to freedom of access to information was created.

²⁶ The Freedom of Information Act is defining entities that are obliged to provide information. These entities are defined in the act in question as obliged persons. List of obliged persons is stated in Section 2 of the Freedom of Information Act.

data. However, in the context of public administration open data, citizens can gather only some data that are collected by public authorities. In this regard, it should be noted that the main idea of the open data regime is that public authorities publish public data automatically and that they can be easily downloaded via the Internet.

Notwithstanding the above, the term open data is stated in *Regulation of Ministry of Finance of the Slovak Republic No. 55/2014 Coll., On standards for public administration information systems* (hereinafter referred to as the "Regulation on Standards"). According to the Regulation on Standards is standard for the indication of data as open data:

"a) provision of data in a dataset²⁷ in the quality of the provided dataset of at least level 3²⁸,

b) provision of data in the open way of use that is fulfilled if:

- 1. the legal aspects of access to data and use of the data are explicitly settled,*
- 2. it is possible to create legal relations for the use of the data via anonymous remote automated access,*
- 3. access to data is made available to all persons under the same conditions while these conditions being explicitly defined,*
- 4. the data may be used for non-commercial and commercial purposes and may be combined with other data, added, corrected, modified or used from the dataset without the obligation to use other dataset data,*
- 5. the activities under the fourth point are free of charge."²⁹*

If the dataset contains at least one open data, it is referred to as a dataset with open data.³⁰

The dataset catalog of public administration can be found on the Open Data Portal, created under the Open Government Initiative. The goal

²⁷ Pursuant to Section 2 (r) of the Regulation on Standards is a dataset defined as "a coherent and self-employed group of related data created and maintained for a particular purpose and stored together under the same scheme."

²⁸ Dataset quality levels are divided into 6 levels of quality. Pursuant to Section 51 (1) of the Regulation on Standards is the dataset at level 3 considered as a dataset that is available in the web environment, the content of the dataset is structured to allow automated processing and the dataset is provided in an open format independent of a particular proprietary software.

²⁹ Regulation on Standards, Section 52.

³⁰ Ibid., Section 52 (2).

of the Open Data Portal is to make accessible data and metadata in distance and in a machine-readable form using open standards and public licenses.³¹

The Open Data Portal is part of the Central Public Administration Portal of the Slovak Republic (hereinafter referred to as the “Central Portal”). The Central Portal contains 1382 datasets which were published by 63 organizations.³²

In the Global Open Data Index survey that examines the openness of government data from all countries of the world, the Slovak Republic took the 32nd place.³³ At EU level, the degree of disclosure of open data is examined within the Digital Economy and Society Index (DESI). The Slovak Republic took in 2016 as part of this evaluation in terms of the open data criterion the 21st place among all EU countries.³⁴

2.6 THE FUTURE OF OPEN DATA IN THE SLOVAK REPUBLIC

The purpose of this subchapter is neither comprehensive comparison of the open data issue in the Slovak Republic and the Czech Republic nor implementation of PSI Directive into Slovak and Czech legal order. We are aiming at pointing out main legal differences regarding the issue of open data, especially its legal definition.

The Government of the Slovak Republic adopted the Action Plan of the Initiative for Open Government in the Slovak Republic for 2017–2019 (hereinafter referred to as the “Action Plan 2017–2019”) at its meeting on 1 March 2017. Open Information is one of the priorities of the Action Plan 2017–2019. Other priorities are open education and open science, government open to dialogue and open justice and public prosecution.

Open data is one of the strategic priorities of the National Concept of Informatization of Public Administration of the Slovak Republic for the years 2016–2020 (hereinafter referred to as the “National Concept 2016”)³⁵. The National Concept 2016 clarifies that

³¹ Available from: <https://data.gov.sk/about> [Accessed March 2018].

³² Available from: <https://data.gov.sk/> [Accessed 6 March 2018].

³³ Available from: <https://index.okfn.org/place/> [Accessed 18 September 2018].

³⁴ Available from: <https://ec.europa.eu/digital-single-market/en/scoreboard/slovakia> [Accessed 6 March 2018].

³⁵ Available from: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25951> [Accessed 6 March 2018].

“the basic type of released data is so-called public sector information that public authorities create, collect or pay for it.”³⁶

The National Concept 2016 proposes the adoption of the Open Data Act which would regulate both the issue of licensing as well as restrictions on the provision of certain public administration data.³⁷ According to the Open Data Strategic Priority which specifies the goals of the National Concept 2016 in the field of open data, it should be an act that transposes the PSI Directive in a clear manner. In our opinion, the adoption of a comprehensive act that would regulate the issue of open data is not the only appropriate solution.

Open data legislation in the Czech Republic could serve as an example for the Slovak Republic. The issue of open data is regulated by Act No. 106/1999 Coll., On Free Access to Information, as amended (hereinafter referred to as the “Czech Freedom of Information Act”). The open data regime was created by amendment of the Czech Freedom of Information Act in 2017.³⁸ The purpose of this amendment was to

“ensure the simplest, reusable use of data provided by the public sector as open data for the creation of commercial and non-commercial services by the professional public.”³⁹

The new legal framework also contains the legal definition of the term open data. According to the Czech Freedom of Information Act, open data is defined as

“information disclosed in a way allowing remote access in an open and machine-readable format when neither manner nor purpose of re-use is limited and which are recorded in the national catalog of open data.”⁴⁰

Information from registries or lists held or managed by public authorities which are lawfully accessible to anyone and can be used for commercial or other profitable activities, for study or for scientific purposes or for public inspection of public authorities shall be disclosed as open data.

³⁶ The National Concept 2016, p. 45.

³⁷ Ibid.

³⁸ Czech Freedom of Information Act. [online] Available from: <http://www.senat.cz/xqw/xervlet/pszenat/htmlhled?action=doc&value=80874> [Accessed 8 March 2018].

³⁹ Statement of reasons of the act that amended Czech Freedom of Information Act [online]. Available from: <https://www.psp.cz/sqw/text/orig2.sqw?idd=112562> [Accessed 9 March 2018].

⁴⁰ Czech Freedom of Information Act, Section 3 (11).

The data in question is recorded in the national catalog of open data⁴¹ which is an information system of the public administration and operated by the Ministry of the Interior of the Czech Republic.⁴²

The list of information to be published as open data is defined in the implementing legal regulation, in particular, the Government Order No. 425/2016 Coll., On the list of information published as open data.⁴³

2.6.1 OPEN DATA REGIME V. PSI RE-USE REGIME V. FREE ACCESS TO INFORMATION REGIME

In general, we could say that open data is special type of PSI made available to public. The European Commission defines open (public) data as

*“PSI that can be readily and widely accessible and re-used, sometimes under non-restrictive conditions.”*⁴⁴

From the perspective of Slovak legal order, especially Freedom of Information Act, we can find some differences between the open data regime and PSI regime and the traditional regime of free access to information.⁴⁵ The main distinguishing characteristics are the purpose of the regime, the scope of released information, periodicity of information releasing and the requirement of application submission.

⁴¹ Available from: <https://portal.gov.cz/otevrena-data/datove-sady/2018-01> [Accessed 9 March 2018].

⁴² Czech Freedom of Information Act, Section 4b (2) and Section 4c.

⁴³ Government Order No. 425/2016 Coll., On the list of information published as open data. [online] Available from: <http://www.epi.sk/zzcr/2016-425> [Accessed 9 March 2018].

⁴⁴ Digital single market open data. [online] Available from: <https://ec.europa.eu/digital-single-market/en/open-data> [Accessed 20 September 2018].

⁴⁵ Following the successful transposition of PSI Directive into the Slovak legal order, three categories of providing information can be mentioned: (I) mandatory disclosure of information (Section 5), contracts (Section 5a), invoices and orders (Section 5b), (II) disclosure of information on request (Section 14 et seq.), (III) disclosure of information for re-use purposes (Section 21b et seq.). Clear legal obligation to disclose PSI as open data is absent in Slovak legal order. In accordance with aforementioned, we can distinguish between free access to information regime (I and II), PSI re-use regime (III) and open data regime. The main idea of defining separate open data regime is the fact that the regime in question is based on disclosure of information in datasets that are available online where no request is required in comparison to PSI re-use regime. Furthermore, on the basis of aforementioned, we could say that Freedom of Information Act regulates providing of information by publishing (I) and providing information on request (II and III). It is necessary to point out that in the case of disclosure of information for re-use purposes (III) is obliged person obliged to make the information available for re-use purposes on request. However, pursuant to Section 21d (1) of the Freedom to Information Act, information for re-use may be disclosed by the obliged person without a request. The Czech Freedom to Information Act regulates providing information by disclosure (Section 4b) and providing information on request (Section 4).

It should be borne in mind that in the case of the free access to information regime, the purpose is achieving transparency and increasing control in public administration. The main aim of the regime in question is the realization of the right to information. The PSI re-use regime is aimed at achieving a commercial objective.⁴⁶ Moreover, the PSI re-use regime can be considered as the realization of the right to business.⁴⁷ In the case of open data regime, despite the undeniable economic potential of public administration data, open data fosters participation of citizens in political and social life and increases transparency of government and public control. Furthermore, having more data openly available will help discover new and innovative solutions to address societal challenges.⁴⁸

Other differences are the scope of released information, the periodicity of information releasing as well as the requirement of application submission. In the case of the free access to information regime, the information is made available one-time and irregularly. Furthermore, a person has to submit an application to access the information. On the other hand, in the case of PSI re-use regime, the disclosure of the information is regular and vast amount of information is provided. A person usually has to submit an application to obtain information for re-use purposes.⁴⁹ In the case of open data regime, the emphasis is placed on the publication of entire datasets of public authorities and these datasets are still available on the Internet. The submission of application is not required.

2.6.2 THE FORMAT OF PROVIDED INFORMATION

One of the most serious obstacles why PSI cannot be published as open data is the structure of information that is released for re-use purposes. Public sector bodies are advised to release documents in available formats or languages.⁵⁰ Where appropriate and possible, the documents in question

⁴⁶ Janssen, K. (2011). The influence of the PSI directive on open government data: an overview of recent developments. *Government. Information Quarterly*, 28, pp. 453.

⁴⁷ Myška, M. et al. (2014) *Veřejné licence v České republice*. Brno: Masarykova univerzita, pp. 97–98.

⁴⁸ Digital single market open data. [online] Available from: <https://ec.europa.eu/digital-single-market/en/open-data> [Accessed 20 September 2018].

⁴⁹ Pursuant to Section 21d (1) of the Freedom of Information Act, information for re-use purposes can be disclosed by the obliged persons without a request.

⁵⁰ PSI Directive 2013, Article 5 (1).

should be made available in an open, machine-readable format along with their metadata.

Documents, as well as metadata, should, to the fullest extent possible, meet official open standards. These standards have been established in writing and contain detailed specifications how interoperability of software has to be ensured. The specifications in question are freely available.⁵¹

A document in a machine-readable format can be considered a document if it is in a file format structured so that software applications can easily identify, recognize, and extract specific data from the document. In terms of machine-readable format, it can be open format or subject to ownership. In the case of an open format, it is meant as file format that is publicly available without any restriction that would prevent re-use. The machine-readable format may also be formally standardized or not.⁵² At present, in the field of open data, technologies are introduced that allow the interconnection of data from different sources to create open interconnected data. In the light of aforementioned, the Resource Description Framework (RDF) format is used. Another recommended format is XML format. It should be noted that Portable Document Format (PDF) is an open standard but is not machine-readable and is therefore not suitable as an open data format.⁵³

Public sector bodies are not obliged to create or adapt documents or provide extracts in order to ensure that documents are in a machine-readable format where this would involve disproportionate effort, going beyond a simple operation.⁵⁴

In accordance with the Freedom of Information Act, the form and method of making the information available for re-use depend on the technical conditions of the public authority. The legislator explicitly prefers the electronic form of disclosure and it is possible and appropriate as open data⁵⁵ allowing automated processing⁵⁶ with their metadata.

⁵¹ Ibid., Article 2 (8). The open standard is characterized by the fact that it does not belong to anyone and can be used by everyone. In particular, we can consider as open standard: XML (eXtensible Markup Language), CSV (Comma Separated Values), JSON (Javascript Object Notation).

⁵² PSI Directive 2013, Recital 21.

⁵³ More on the issue of open interconnected data in Geiger, CH., P., Von Lucke, J. (2012) Open Government and (Linked) (Open) (Government) (Data). *JeDEM Vol. 4, No. 1*, pp. 265–278.

⁵⁴ PSI Directive 2013, Article 5 (2).

⁵⁵ Regulation on Standards, Section 52.

⁵⁶ Ibid., Section 51 (2).

The disclosure of information for the purpose of its re-use arranged in a structure or formats according to the criteria specified by the applicant is not an obligation of the public authority. If the requirements of the applicant go beyond the simple operation, the public authority is not obliged to provide a specific technical solution for the connection or connection of the applicant. Furthermore, public authority is not obliged to continue the preparation and storage of information for the purpose of its re-use through another person.⁵⁷

The Czech Freedom of Information Act states that public authorities are obliged to disclose specific types of information⁵⁸ as open data. Such an obligation is absent in the case of the Slovak Freedom of Information Act. According to the the Czech Freedom of Information Act, specific information have to be disclosed in an open and machine-readable format.⁵⁹ Open format is defined as

*“the format of a data file that is not dependent on specific technical and software equipment and is made available to the public without any restriction that would make it impossible to use the information contained in the data file.”*⁶⁰

Machine-readable format is defined as

*“format of a data file with a structure that enables software to easily find, recognize and extract from that data set specific information, including individual data and their internal structure.”*⁶¹

In connection with the format of information provided on request, the Czech Freedom of Information Act states that the information is provided in the formats and languages according to the content of the request for information, including the relevant metadata unless otherwise provided in the act in question. However, the obliged entity⁶² is

⁵⁷ Freedom of Information Act, Section 21g (2).

⁵⁸ Information from registries or lists held or managed by public authorities which are lawfully accessible to anyone and can be used for commercial or other profitable activities, for study or for scientific purposes or for public inspection of public authorities. Section 4b (2) of the Czech Freedom of Information Act.

⁵⁹ Czech Freedom of Information Act, Section 3 (11).

⁶⁰ Ibid., Section 3 (8).

⁶¹ Ibid., Section 3 (7).

⁶² Obligated entities are defined in Section 2 of the Czech Freedom of Information Act. Entities in question are obliged to provide information according to the Czech Freedom of Information Act.

not obliged to change the format or language of the information or to create metadata for information if such a change or the creation of metadata would be an unreasonable burden for the obliged entity. In this case, the obliged entity will comply with the request by providing information in the format or language in which it was created.⁶³ In addition, if possible, taking into account the nature of the application submitted and the manner of recording the information requested, the obliged entity will provide the information in electronic form.⁶⁴

3. PROCESSING OF OPEN DATA AFTER GDPR

PSI in form open data facilitate free flow of information within public space. Respected datasets are comprised of non-personal and personal data. When data reveal any information related to an identified or identifiable individual, another piece of legislation plays an important role.

Protection of personal data is in the center of interest of politicians, academics and practicing lawyers in these days. The main reason for the buzz is the reform of data protection framework. The leading legal instrument in the area is adopted *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 – hereinafter referred to as the “GDPR”)*⁶⁵, coming into force on 25th May 2018. Second part of the EU data protection reform package constitutes of *directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. The emphasis in this article is put solely on GPDR as a basic legal instrument governing data protection law in society.

⁶³ Ibid., Section 4a (1).

⁶⁴ Ibid.

⁶⁵ 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). *Official Journal of the European Union* (L 119/1) 4 May. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

This part of the article aims at data protection issues related to the processing of personal data that has been made public and re-use of published public sector information including personal data. First of all, it is of the essence to make the distinction between two potential options of publication of PSI as open data: (a) anonymized datasets or (b) datasets that include personal data (including pseudonymized datasets). If datasets are truly anonymized and it is not possible to e.g. via reverse identification to determine a person whom personal data are processed, the GDPR does not apply.⁶⁶ On the other hand, if published datasets contain information that are “relating to an identified or identifiable natural person”, data protection laws apply and controllers and processors (entities processing personal data) shall comply with specific obligations laid down by GDPR. The same shall be held considering pseudonymized data. Pseudonymization may be defined as

“replacing one attribute (typically a unique attribute) in a record by another.”⁶⁷

Pseudonymization is just a security measure to foster security of personal data processing. Although identification of individual is impeded, it is still possible due to unique key individualizing an identified individual.

Secondly, the distinction between first controllers and re-users⁶⁸ has to be made due to different issues connected with processing of personal data. First controllers are discussed only briefly and deeper analysis is made regarding potential re-users of open data as specific legal grounds for re-using of publicly available information is not provisioned in national laws of Slovak Republic and Czech Republic after GDPR.

⁶⁶ See 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). *Official Journal of the European Union* (L 119/1) 4 May. Recital 26. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

⁶⁷ Article 29 Data Protection Working Party 05/2014 on Opinion on Anonymisation Techniques, supra note 228, p. 20. [online] Available from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 10 August 2018].

⁶⁸ Terms are used in line with outcomes of LAPSI Policy Recommendation No. 4: Privacy and Personal data protection – LAPSI Working Group 2 Privacy aspects of PSI. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366 [Accessed 10 August 2018].

3.1 FIRST CONTROLLERS OF OPEN DATA

Public administration in general collects vast amount of data related to citizens of respective states. In many cases data collected by public authorities includes personal data e.g. related to identity of users of public administration services, sensitive information about health or social security. Furthermore, publicly available registers may contain personal data related to identifiable natural persons that are public officials or in a business relationship with state.⁶⁹

From the personal data protection view, public authorities as first controllers shall be considered the original controllers of personal data. Data are directly (and in most cases voluntarily) provided to public authorities by data subjects. Personal data are collected mainly on legal grounds of legal obligation pursuant to Article 6 (1) c) GDPR as it is directly prescribed by law that public authorities process personal data within their competences or performance of a task carried out in the public interest or in the exercise of official authority in accordance with Article 6 (1) e) GDPR. The processing operation at stake is publishing some of the information and the issue is that using aforementioned legal grounds require (rather specific) provision of law of member state or EU law. It is of our opinion that personal data originally collected for the purpose of fostering transparency may be published with the same purpose in hand. On the other hand, consequences and effects on rights and freedoms have to be taken carefully into account and that might result in limited (either by scope or use) publication of personal data by public authorities.⁷⁰

Balancing right to privacy and/or right to data protection and public interest via publication of information related to identifiable individuals is subject of debates not only within academics.⁷¹ The issue is partially reflected in recital 154 GDPR.⁷² After all, the European Court of Human Rights in case concerning publication of data of elected local councilor stated that

⁶⁹ E.g. *Register of Public Sector Partners in Slovak Republic*. [online] Available from <https://rpvs.gov.sk/rpvs> [Accessed 10 August 2018].

⁷⁰ See more in Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal*. 30, pp. 2073–2132.

⁷¹ See e.g. outcomes of LAPSI 2.0 Thematic Network – D2.2 – Position paper access to data. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8341 [Accessed 10 August 2018].

“the general public has a legitimate interest in ascertaining that local politics are transparent and Internet access to the declarations makes access to such information effective and easy. Without such access, the obligation would have no practical importance or genuine incidence on the degree to which the public is informed about the political process.”⁷³

Therefore such processing operations require careful assessment of proportionality and balancing exercise.

Besides that, controllers including public authorities have to be in compliance with principles of processing of personal data as provisioned in Article 5 GDPR,⁷⁴ specific security and organizational measures have to be effectively implemented e.g. obligatory appointment of data protection officer.⁷⁵

Concluding this section, public authorities are in better position from data protection perspective than potential re-users. The latter stems from the fact that public authorities are original controllers (original collectors) of personal data and legal exercise of public power delegated by law provides justification for fostering transparency in public administration by making relevant data publicly available.

⁷² *“This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council (14) leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.”*

⁷³ *Wypych v. Poland*, No. 2428/05, ECHR 2005 (Admissibility decision).

⁷⁴ For more elaborate discussion of issues connected to application of principles of data protection see Borgesius, F.Z., Gray, J., Eeouch, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal*. 30, pp. 2073–2132.

⁷⁵ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 37 (1) a). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

3.2 RE-USERS OF OPEN DATA

“After GDPR era” caught controllers and processors of open data in the role of users or re-users, i.e. persons different from original controllers that made data publicly available in precarious situation. The reason is that GDPR does not explicitly provision further processing of personal data for re-use and implicitly left the issue for national legislators.

The question is particularly important for various non-governmental organizations (NGOs) and other bodies governed by the private law that serve as watchdogs of the government or public administration in general. When it comes to re-use of PSI (open data), national data protection acts traditionally offer a legal ground for further processing of PSI (open data). However, it seems that at least considering Slovakia, the game has changed. Slovak New Data Protection Law⁷⁶ does not contain the exception for processing of personal data that has already been published. Thus, the question arose: Is further processing of PSI particularly in form of open data dead for entities from private sector willing to participate in the public sphere?

3.2.1 PURPOSE OF RE-USE OF OPEN DATA FROM THE DATA PROTECTION PERSPECTIVE

Each processing operation with personal data needs to have a purpose and a legal ground. The aforementioned aspects are “alfa” and “omega” of data protection and are closely connected in a sense that each purpose shall be covered by one of the legal grounds. As mentioned in the previous parts of the article, the main purpose of open data is to ensure and promote transparency in public administration and increase the participation of citizens in the context of public matters.⁷⁷ Thus the primary aim of the discussed concept shall be perceived as broadly as possible due to its nature. However, using vague terms especially considering purpose specification for processing of personal data is a rather sensitive issue.

⁷⁶ Slovak Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts. Slovakia.

⁷⁷ Taking into account Open Data interests as defined by Borgesius et. al the interest would fall within category of „political accountability and democratic participation.“ Two other interests are innovation and economic growth and public sector efficiency and service delivery. See Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal*, 30, pp. 2078–2084.

The question of purpose specification is analyzed in Working Party 29 (hereinafter referred to as the “WP29”) Opinion on “purpose limitation”.⁷⁸ GDPR stipulates that personal data shall be

“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”⁷⁹

The problem at stake is how to define the purpose of PSI in form of open data to be in compliance with requirements to be specific, explicit and legitimate.

The specification of the purpose lies in the requirement of a controller to determine how the processed personal data will be used for and assess the volume of personal data necessary for the processing operation. According to the Opinion of WP29

“the purpose of the collection must be clearly and specifically identified [...] (and) [...] it must be detailed enough to determine what kind of processing is and is not included within the specified purpose.”⁸⁰

When it comes to the concept of open data, the provision of the wording of the purpose is challenging issue. a notice declaring that “*Your personal data may be used in public interest*” may not suffice as the declaration is too vague. What is more, the legal definition of public interest does not exist and the interpretation of pertinent notion continually changes through time and space. In our opinion, the emphasis shall be put on the purpose of the original processing operation resulting in the publication of pertinent information.

The second requirement of compliance with the principle of purpose specification is explicitness of the purpose. In layman’s words, the purpose

⁷⁸ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018]. The opinion is generally still applicable under GDPR as per the fact that from material point of view deals with principle of purpose limitation that is preserved in new regulation.

⁷⁹ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (1) (b). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

⁸⁰ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 15. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 3 March 2018].

of the processing operation shall be openly and clearly stated by available means. According to the OECD

“such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licenses provided by supervisory bodies.”⁸¹

Taking into account the nature of the concept of open data, the original purpose of the collection is provided by specific legislation or via other legal ground. Persons entering public domain shall reasonably expect re-publication and further use of their personal data once provided for the purpose of public control and transparency of public governance. What is more, if a person publishes his personal data as an obligation provided by law, further publication (in terms of re-use) of pertinent data for the same or similar purpose⁸² should be deemed compatible with the requirement of a reasonable purpose.

Thirdly, the purpose must be legitimate. The legitimacy of the purpose may be perceived in two manners. On one hand, the purpose must be based on one of six legal grounds provided by the data protection legislation being consent, the performance of the contract, legal obligation, vital interest, public interest and legitimate interest. On the other hand, for the purpose to be legitimate compliance with aforementioned duty is not enough. The purpose as such shall be in accordance with the law in general. According to the WP29, the law

“includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such ‘law’ would be interpreted and taken into account by competent courts.”⁸³

⁸¹ Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Section 54. [online] Available from: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#memorandum> [Accessed 3 March 2018].

⁸² 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 6 (4). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

⁸³ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 20. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

Re-use of open data concerning government and public authorities shall be considered in accordance with the law due to the nature of the activity as promoting transparency and participation of the citizens in public administration affairs. The aforementioned is in line with the idea of openness of public administration and “sousveillance”⁸⁴ as a method of control of the government executed by society.

The principle of purpose specification is constituted by two aspects – (i) specification of a purpose per se and (ii) compatibility test. The compatibility test is provisioned in Article 6 (4) of the GDPR.⁸⁵ In other words, if you process personal data and the purpose of the original processing operations changes, there is an obligation to find a new legal ground. However, if the new purpose is compatible with the original purpose, search for a new legal ground is not necessary. GDPR states five factors that shall be taken into consideration while assessing compatibility: (i) any link between your initial purpose and the new purpose, (ii) the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect, (iii) the nature of the personal data – e.g. is it special category data or criminal offence data, (iv) the possible consequences for individuals of the new processing and (v) whether there are appropriate safeguards – e.g. encryption or pseudonymisation.⁸⁶

It shall be emphasized that two strict limitations exist for using compatible purpose in general. First of them is explicitly mentioned in the GDPR stating that compatibility test does not apply to the (original) processing based on a consent as a legal ground. Secondly, a third party that is not an original controller conducting processing operations shall carefully follow the original purpose that had been specified. As WP29 notes:

⁸⁴ Mann, S. (2004). *Sousveillance: Inverse Surveillance in Multimedia Imaging*. *Computer Engineering*, pp. 620–627. [online] Available from: http://wearcam.org/acmmm2004_sousveillance/mann.pdf [Accessed 3 March 2018].

⁸⁵ „Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected.”

⁸⁶ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 6 (4). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

“the mere fact that personal data are publicly available for a specific purpose does not mean that such personal data are open for re-use for any other purpose.”⁸⁷

Illustrating aforementioned on the example, in many countries it is obligatory for government officials to publish their asset declarations.⁸⁸ On one hand, it would be potentially compatible to gather all publicly available information and create a profile of a specific government official including tax return data to facilitate the transparency. On the other hand, using personal data in tax returns for sending commercial advertisements by a car reseller based on tax revenues would not be probably deemed compatible with the original purpose.

Coming back to the open data and re-use, the WP29 seems to be aware of challenges of the discussed institutes and calls for cautious impact assessment. It particularly notes that

“once personal data are publicly available for re-use, it will be increasingly difficult, if not impossible, to have any form of control on the nature of potential further use, be it for historical, statistical, scientific or other purposes.”⁸⁹

Although the WP29 prefers to conduct anonymization techniques in disseminating personal data to the public sector for re-use, the anonymization would kill the purpose and task of open data as defined at the beginning of the article.

Concluding findings above the compatibility test of a purpose is not completely appropriate measure to use as a basis for processing of personal data in the context of re-use of open data by third parties e.g. NGOs acting as watchdogs of activities of public bodies.

⁸⁷ Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information (PSI) reuse, p. 20. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018]. As this opinion deals with basic issues with processing of open data from the data protection point of view it shall be applicable to certain extent also under GDPR.

⁸⁸ See Djankov, S. – La Porta, R. – Lopez-de-Silanes, F. – Schleifer, a (2009). Disclosure by Politicians. *American Economic Journal: Applied Economics*, *American Economic Association*, vol. 2(2), pp. 179–209.

⁸⁹ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 49. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

3.2.2 POTENTIAL LEGAL GROUNDS IN GDPR AND SLOVAK AND CZECH DATA PROTECTION ACTS

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.⁹⁰ Lawfulness of processing is developed in the Article 6 of GDPR explicitly stipulating legal grounds for processing of personal data (consent, the performance of the contract, legal obligation, vital interest, public interest and legitimate interest). WP29 in its opinion 06/2013 on open data and public sector information re-use also highlights that any further re-use must have an appropriate legal basis.⁹¹ Taking into account re-use of PSI in form of open data legal grounds of the interest are public interest and legitimate interest.⁹² This part of the article analyzes aforementioned legal grounds from the view of re-use of open data.

a) public interest

Article 5 (1) (e) GDPR stipulates that processing of personal data is lawful when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The legal ground “public interest” contains two different scenarios where first is designed to govern processing operations with personal data of official authority as a controller and the second scenario anticipates tasks in (delegated) public interest conducted by private bodies. However, GDPR sets forth one limitation for using discussed legal ground for processing. The basis for the processing under the legal ground of public interest shall be laid down by Union law or Member state law to which a controller is subject.⁹³ In other words, a special law that provides the purpose of such

⁹⁰ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, p. 49. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 3 March 2018].

⁹¹ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (1) a). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

⁹² Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information (PSI) reuse, p. 19. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018].

⁹³ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (3). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

processing, potential data subjects and types of personal data processed is needed. It is of the essence to note that many NGOs monitoring public servants or government officials are not established by specific acts but rather as entities regulated by private law and completely independent from the state. Deriving from this it may prove very challenging to argue a public interest as a lawful ground for processing personal data in the context of re-use of open data.

b) legitimate interest

According to the Article 6 (1) (f) processing shall be lawful if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Compliance with the aforementioned legal ground for processing requires so-called “balancing test” sketched in Recital 47 of the GDPR. The legal ground of legitimate interest shall not be applied to processing carried out by public authorities in the performance of their tasks.

Taking into account the Opinion 06/2014 on the notion of legitimate interests of the data controller (hereinafter referred to as the “Opinion”) drafted by Working Party 29 the interest shall be legitimate and legitimacy is embedded *inter alia* in exercise of the right to freedom of expression or information, including in the media and the arts and prevention of fraud, misuse of services, or money laundering.⁹⁴ The latter at least partially covers purposes of open data. The Opinion introduces four factors to be evaluated during the balancing test. It is of the essence to analyze (i) the controller’s legitimate interest, (ii) impact on the data subjects, (iii) provisional balance and (iv) additional safeguards applied by the controller to prevent any undue impact on the data subjects.⁹⁵ Thus the analysis of these factors in the context of re-use of open data is necessary.

⁹⁴ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 25. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

⁹⁵ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 33 and further. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

When it comes to the *first factor*, WP29 explains that legitimate interest can stem from exercising of a fundamental right, public interest (interests of the wider community) or other legitimate interest. The European Charter of Fundamental Rights provisions Right to good administration in the Article 41. Due to the wording of pertinent article

*“every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices, and agencies of the Union.”*⁹⁶

The authors of the article are of the opinion, that the Right to good administration shall not be perceived only as a basis for a wide range of procedural rules. The relevant right may be also understood as a general obligation of a state to provide effective public administration that is closely connected to the transparency and accountability. Deriving from this, re-use of open data including personal data of government officials shall fall within the discussed right. It is also of the essence to note that in case of inability to rely on the exercise of human right as a basis for legitimate interest, the whole idea of open data and re-use in general related to public governance is definitely in public interest or the interests of the wider community as described in the Opinion. WP29 even explicitly uses the example of processing personal data by a non-profit organization in order to raise awareness of government corruption.⁹⁷

The second factor of the balancing test is the analysis of the impact on data subjects. Aspects to be taken into consideration are the nature of personal data, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject.⁹⁸ Generally, the assessment of the impact should be perceived in a broad way to evaluate potential and actual threats to the freedoms and rights of data subjects including positive and negative consequences.

⁹⁶ Article 41 *Charter of Fundamental Rights of the European Union*, 26 October 2012 (2012/C 326/02). [online] Available from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12012P%2FTXT> [Accessed 18 August 2018].

⁹⁷ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 35. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

⁹⁸ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 36. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

However, specificity of open data is that pertinent data have already been published and processed on other legal ground (typically consent or statutory obligation) and therefore the data subject concerned shall be already aware of potential further processing operations. The requirement to assess the nature of the data reflects the dichotomy in the typology of personal data being personal data⁹⁹ and sensitive personal data¹⁰⁰. As WP29 notes in the Opinion, it is also relevant if the data has already been made publicly available.

“The fact that personal data is publicly available may be considered as a factor in the assessment, especially if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability).”¹⁰¹

In case of open data the purpose of re-use is clearly in transparency and creating a public-friendly interface containing pertinent information and thus such processing operation with personal data shall be considered legitimate considering the nature of the data processed. Another aspect is the way data are being processed. In other words, it is of the essence to evaluate how data are processed, e.g. if there is profiling, commercial profit, deep-packet inspection or predictions about data subjects are made. Again, it shall be emphasized that re-using of publicly available information in form of open data is just “processing of already processed”. In this case, if data are already in the public sphere (online or in publicly available registers) it would be inappropriate to sanction controllers or processors for

⁹⁹ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 4 (1). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

¹⁰⁰ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 9 (1). [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018]: “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”

¹⁰¹ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 39. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

further processing in the (identical) public sphere. The same applies to the reasonable expectations of the data subject. Once data of persons concerned is published, it is reasonable to expect that data will be re-used or processed for the same purpose. On the other hand, any commercial profit from further processing operations deriving from open data may be considered as a crucial factor in assessing whether the interest of the controller is legitimate although WP29 notes that

“the assessment of compatibility should not be primarily based on whether the economic model of a potential re-user is based on profit or not.”¹⁰²

Nevertheless, the close connection of re-using personal data would probably be a strong indication of incompatibility of processing operations. Lastly, it is important to weight status of the data controller and data subject. In case of re-use of publicly available information the “clash” is between government officials, politicians or highly ranked public servants (and sometimes their relatives) and non-governmental organizations conducting their activity without the help of public sector. The specific nature of the relationship sketched above shall be taken into account with regard to public interest.

The third factor to be considered is to carry out provisional balancing. the WP29 especially notes to include requirements of transparency and proportionality in the conducting provisional balancing. Put differently, adherence to the compliance with data protection rules

“should mean that the impact on individuals is reduced, that data subjects’ interests or fundamental rights or freedoms are less likely to be interfered with and that therefore it is more likely that the data controller can rely on”¹⁰³

legitimate interest as a legal ground for processing.

The fourth factor in assessing whether the interest of the controller is legitimate lies in providing additional safeguards applied by the controller.

¹⁰² Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information (‘PSI’) re-use, p. 21. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf [Accessed 3 March 2018].

¹⁰³ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 41. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

In cases where the impact on the data subjects is more severe or significant, the more attention shall be given to applying additional safeguards. WP29 illustrates additional safeguards *inter alia* on the examples of strict limitations of a quantity of data collected or strict application of data minimization principle.¹⁰⁴ With regard to novelties of GDPR, it may be also of the essence to consider the use of data protection by design and data protection by default philosophies that are relevant for further processing of open data.

Another point in favor of using a legitimate interest as the legal ground for further processing of personal data is an example¹⁰⁵ drafted by WP29 describing a scenario where NGO republishes expenses of Members of Parliament. The expenses are published in the context of statutory obligation and NGO analyses and re-publishes the data in more informative and public-friendly way.

“Assuming the NGO carries out the re-publication and annotation in an accurate and proportionate manner, adopts appropriate safeguards, and more broadly, respects the rights of the individuals concerned, it should be able to rely on”¹⁰⁶

legitimate interest as a legal ground for processing. What is more, the fact that data has already been published weighs in favor of the legitimacy of the processing operations together with the reasonability of expectations of the data subjects. The balance between the legitimacy of the processing operation and impact on rights and freedoms of data subjects shall even be withheld the situations where criminal investigations or loss of elections are a consequence of re-publishing the data concerned. It is also essential to add that it is not relevant on which legal ground the original processing of personal data is conducted as all of them are equal from the point of data protection law.

¹⁰⁴ Ibid., p. 42.

¹⁰⁵ Ibid., p. 57.

¹⁰⁶ Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 41. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].

c) potential legal grounds in Slovak Data Protection Act and Czech Data Protection Act

As mentioned earlier in the article, during the transposition of the old directive on personal data¹⁰⁷ many member states chose to implement specific provisions creating a legal ground for processing publicly available information. It shall be noted that GDPR leaves space for Member states to provide specific provisions in their national laws concerning balancing right to data protection and right to freedom of expression and free access to documents.¹⁰⁸

Slovak act No. 122/2013 Coll., On Protection of Personal Data states that

“the controller shall process personal data without the data subject’s consent also if processed personal data have already been disclosed pursuant to Law and the controller properly marked them as disclosed.”¹⁰⁹

The aforementioned provision shall be deemed to be statutory legal ground for processing that has been widely used by NGOs in the context of further re-using of open data. However new Slovak Data Protection Act¹¹⁰ does not contain such legal ground for processing with regard to re-use of publicly available information. According to authors of the article entities may rely on Section 78 (2) of Slovak Data Protection Act that provides an exception establishing that the controller shall process personal data without the data subject’s consent also, if processing of personal data is necessary for needs of informing the society via mass media and if processing of personal data is conducted by the controller that has such informing in the object of its activity.¹¹¹ In other words, if NGO is set up as a watchdog of government officials or evaluating financial transactions

¹⁰⁷ Directive 95/46/EC of the 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. *Official Journal of the European Union* (1995/L 281/31) 23 November. [online] Available from: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN:PDF> [Accessed 3 March 2018].

¹⁰⁸ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 85 and 86. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

¹⁰⁹ *Slovak act No. 122/2013 Coll., On Protection of Personal Data and on changing and amending of other acts*, resulting from amendments and additions executed by the Act. No. 84/2014 Coll., Slovakia. Section 10 (3) (e).

¹¹⁰ *Slovak Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts*. Slovakia. (Translation by Office for the protection of personal data of Slovak Republic).

in public funding (or any other open data), it would be possible to argue that informing the society via the Internet may be within the range of the statutory legal ground described above.

A similar provision in Czech Data Protection Act No. 101/2000 Coll. is allowing (that)

*“the controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data... if they were lawfully published in accordance with special legislation”.*¹¹²

However, situation under proposal of new Czech Data Protection Act is different. Although this proposal contains exception for processing of personal data for journalistic purposes in section 16 and following, the legislative construction is more specific than e.g. in section 78 (2) of Slovak Data Protection Act due to the fact that journalistic purposes are explicitly mentioned and does not leave place for discretion (unlike in case of informing society via mass media). Seizing the “Czech” exception for re-use of open data is therefore more than questionable.

3.2.3 FURTHER GDPR CHALLENGES AND IMPACT OF THE PROCESSING

Even if a private body relies on one of the legal grounds for processing together with the fulfillment of requirements for purpose specification, it will be challenging to be in compliance with obligations laid down by GDPR. In this part of the article, The brief discussion of selected obligations shall take place.

First issue is connected to the principle of accuracy. The principle of accuracy means that personal data that are subject to the processing operation shall be accurate and, where necessary, kept up to date. What is more, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.¹¹³ In case of re-using open data the controller shall monitor the original source of data. Establishing

¹¹¹ Slovak Act No. 18/2018 Coll., *On Protection of Personal Data and on Changing and amending of other acts*. Slovakia. (Translation by Office for the protection of personal data of Slovak Republic). Section 78 (2). (Translation by Matúš Mesarčík).

¹¹² Czech Act No. 101/2000 Coll., *On the protection of personal data and on the amendment on some acts*. Czech Republic. Section 5 (2) (d). (Translation by Office for the protection of personal data of Czech Republic).

a monitoring mechanism would be an essential according to the obligations in GDPR. Assessing the accuracy of huge amounts of datasets might be an onerous requirement for small entities acting as watchdogs.

Second issue is rights management. Data subjects have specific rights provided directly by GDPR. Controllers are obliged to be in compliance with management of motions and claims of data subjects concerning their rights. Taking into account that re-using of open data is usually made without knowledge of data subjects, it is absolutely necessary to adhere with the informational obligation of the controller where personal data have not been obtained from the data subject.¹¹⁴ It has to be added that the Article 14 does not apply *inter alia* where the data subject already has the information (related to the processing of personal data) or the provision of such information proves impossible or would involve a disproportionate effort. GDPR states that

“in that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.”¹¹⁵

In the context of re-use of open data it really might occur that especially number of data subjects is high. According to the WP29

“the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.”¹¹⁶

The example stated in this part of the article emphasizes challenges adhering to the rights management in compliance with GDPR might be for

¹¹³ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 5 (1) d. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

¹¹⁴ 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). *Official Journal of the European Union* (L 119/1) 4 May. Art. 14. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

¹¹⁵ 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). *Official Journal of the European Union* (L 119/1) 4 May. Recital 62. [online] Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 3 March 2018].

¹¹⁶ Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679, p. 27. [online] Available from: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 [Accessed 3 March 2018].

controllers of processing operations with personal data that has already been published.

The issue of compatibility of further processing of open data has already been sketched while assessing purpose and legal grounds. It may be quite challenging for a third party to foresee the initial purpose of the publications and be in compliance with it in further processing operations. What is more, there might be situations where personal data are published only for limited amount of time. In this case, monitoring obligation of a controller shall be emphasized again and take into account potential issues related to lack of accountability.

Although GDPR provides implicit space for re-using of personal data for third parties, some of the issues have been outlined above. The most critical are connected to relying on relevant legal ground and purpose specification.¹¹⁷ It shall be emphasized, that special legal regime (or exception e.g. presented in former Slovak and Czech Data Protection Acts) for processing already published personal data may still be the best option how to deal with uncertainty in processing open data from the data protection view. However, that requires actionability of national legislators and public debate on the topic. The first step has already been taken by European Commission with regard to proposal for a new PSI Directive.¹¹⁸

4. CONCLUSION

The analysis of the term open data and its regime from the perspective of Slovak legal order revealed some deficiencies. First of all, the disclosure of information in electronic form is only preferred and where possible and appropriate, as open data. Clear obligation to publish public administration data as open data is absent. Secondly, the term open data and the scope of disclosed open data is not defined in by generally binding legal act in Slovak legal order.

Open data legislation in the Czech Republic could serve as good example for the Slovak Republic. The Czech Freedom of Information Act

¹¹⁷ For more elaborate discussion on coherency see *Study to support the review of Directive 2003/98/EC on the re-use of public sector information*, pp. 134–140. [online] Available from: <https://publications.europa.eu/en/publication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en> [Accessed 11 September 2018].

¹¹⁸ *Proposal for a revision of the Directive 2003/98/EC on the reuse of public sector information*. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information> [Accessed 11 September 2018].

contains the legal definition of the term open data and the list of information to be published as open data is defined in the implementing legal regulation.

The PSI Directive focuses on the economic aspects of re-use of information rather than on the access of citizens to information. It has no intention to regulate access to information that are held by public sector bodies. Such a situation in connection with the unwillingness of public sector bodies to disclose PSI as open data hinders citizens and entrepreneurs from re-using of PSI for commercial or non-commercial purposes.

GDPR and national data protection acts offer several possibilities how to further conduct processing operations with regard to open data. The most suitable option seems to be careful delineation of the purpose and using a legitimate interest of the controller as a legal ground. However, GDPR challenges such processing of information by imposing strict obligations on the controllers and voices calling for more suitable regime in the context of more coherency may have a point.

LIST OF REFERENCES

- [1] *Act No. 101/2000 Coll., On the protection of personal data and on the amendment on some acts.* Czech Republic. In Czech.
- [2] *Act No. 106/1999 Coll., On Free Access to Information as amended.* Czech Republic. In Czech.
- [3] *Act No. 18/2018 Coll., On Protection of Personal Data and on Changing and amending of other acts.* Slovakia. In Slovak.
- [4] *Act No. 211/2000 Coll., On Free Access to Information and on changes and amendments to certain acts.* Slovakia. In Slovak.
- [5] Action Plan of the Initiative for Open Government in the Slovak Republic for 2017–2019. [online] Available from: https://www.opengovpartnership.org/sites/default/files/Slovakia_NAP_2017-2019_EN.pdf [Accessed 20 September 2018].
- [6] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 3 March 2018].
- [7] Article 29 Data Protection Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 20. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp207_en.pdf

- [Accessed 3 March 2018].
- [8] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 25. [online] Available from: http://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2014/wp217_en.pdf [Accessed 3 March 2018].
- [9] Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, 32 (4), pp. 399–418.
- [10] Borgesius, F.Z., Gray, J., Eechoud, M.V. (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal*, 30, pp. 2073–2132.
- [11] Boseley, S. UK heart operation death rates fall after data published. *The Guardian*. [online] Available from: <https://www.theguardian.com/lifeandstyle/2009/jul/30/heart-surgery-death-rates-fall> [Accessed 20 September 2018].
- [12] *Charter of Fundamental Rights of the European Union*, 26 October 2012 (2012/C 326/02). [online] Available from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A12012P%2FTXT> [Accessed 18 August 2018].
- [13] *Creating value through open data*. [online] Available from: https://www.europeandataportal.eu/sites/default/files/edp_creating_value_through_open_data [Accessed 20 September 2018].
- [14] *Crimereports.com*. [online] Available from: https://www.crimereports.com/agency/santa_cruzpd [Accessed 20 September 2018].
- [15] *Data.europa.eu*. [online] Available from: <https://data.europa.eu/euodp/en/data> [Accessed 20 September 2018].
- [16] *Datasey*. *Data.gov.sk*. [online] Available from: <https://data.gov.sk/dataset> [Accessed 20 September 2018].
- [17] Dawes, S., & Helbig, N. (2010). Information strategies for open government: Challenges and prospects for deriving public value from government transparency. *Electronic Government*, 6228, pp. 50–60.
- [18] *Digital single market – Slovakia*. [online] Available from: <https://ec.europa.eu/digital-single-market/en/scoreboard/slovakia> [Accessed 20 September 2018].
- [19] *Digital single market open data*. [online] Available from: <https://ec.europa.eu/digital-single-market/en/open-data> [Accessed 20 September 2018].
- [20] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. *Official Journal of the European Union*

- (2003/L345/90). 31 December. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32003L0098> [Accessed 3 March 2018].
- [21] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance. *Official Journal of the European Union* (2013/L1751/1) 27 June. [online] Available from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013L0037> [Accessed 3 March 2018].
- [22] Directive 95/46/EC of the 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. *Official Journal of the European Union* (1995/L 281/31). 23 November. [online] Available from: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN:PDF> [Accessed 3 March 2018].
- [23] Djankov, S. – La Porta, R. – Lopez-de-Silanes, F. – Schleifer, A (2009). Disclosure by Politicians. *American Economic Journal: Applied Economics*, American Economic Association, vol. 2(2), pp. 179–209.
- [24] *Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Section 54. [online] Available from: <http://www.oecd.org/sti/economy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm#memorandum> [Accessed 3 March 2018].
- [25] Geiger, CH., P., Von Lucke, J. (2012) Open Government and (Linked) (Open) (Government) (Data). *JeDEM*, Vol. 4, No. 1, pp. 265–278.
- [26] *Global Open Data Index: Survey*. [online] Available from: <http://global.census.okfn.org/> [Accessed 20 September 2018].
- [27] Guidelines on recommended standard licences, datasets and charging for the reuse of documents 2014/C 240/01. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2014.240.01.0001.01.ENG [Accessed 20 September 2018].
- [28] Government Order No. 425/2016 Coll., On the list of information published as open data. Slovakia. In Slovak. [online] Available from: <http://www.epi.sk/zzcr/2016-425> [Accessed 9 March 2018].
- [29] *History – International Open Data Charter*. [online] Available from: <http://opendatacharter.net/history/#> [Accessed 20 September 2018].
- [30] Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European Journal of ePractice*, pp. 1–13.

- [31] Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. *Government. Information Quarterly*, 28, pp. 446–456.
- [32] Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 29, pp. 258–268.
- [33] *KohoVolit.eu*. [online] Available from: <http://kohovolit.eu> [Accessed 20 September 2018].
- [34] LAPSI 2. Thematic Network – D2 – Position paper access to data. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8341 [Accessed 10 August 2018].
- [35] LAPSI Working Group 2 Privacy aspects of PSI. [online] Available from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366 [Accessed 10 August 2018].
- [36] *Legislation.gov.uk*. [online] Available from: <http://www.legislation.gov.uk/> [Accessed 20 September 2018].
- [37] *Live map of London Underground*. [online] Available from: <http://traintimes.org.uk/map/tube/> [Accessed 20 September 2018].
- [38] *London datastore*. [online] Available from: <http://data.london.gov.uk/> [Accessed 20 September 2018].
- [39] Materiál programu rokovania. *Rokovania.sk*. [online] Available from: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25951> [Accessed 6 March 2018].
- [40] Mann, S. (2004). *Sousveillance: Inverse Surveillance in Multimedia Imaging*. *Computer Engineering*, p. 620–627. [online] Available from: <http://wearcam.org/acmmm2004/sousveillance/mann.pdf> [Accessed 3 March 2018].
- [41] Munk, R. (2017) Attempt to increase the transparency. *Bratislava law review*, Vol. 1, No. 2, pp. 167–173.
- [42] Myška, M. et al. (2014) *Veřejné licence v České republice*. Brno: Masarykova univerzita, 192 p.
- [43] National Concept of Informatization of Public Administration of the Slovak Republic for the years 2016–2020.
- [44] *O nás*. *Data.gov.sk*. [online] Available from: <https://data.gov.sk/about> [Accessed 20 September 2018].
- [45] Olejár, D. et al. (2015) *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 175 p.

- [46] *Open Knowledge Foundation: The Open Data Manual* (2011). [online] Available from: <http://opendatahandbook.org/> [Accessed 1 March 2018].
- [47] *Otvorené zmluvy*. [online] Available from: <http://otvorenezmluvy.sk> [Accessed 20 September 2018].
- [48] Polčák, R. (2016) Informace a data v právu. *Revue pro právo a technologie* 7, pp. 67–91.
- [49] *Portál veřejné správy*. [online] Available from: <https://portal.gov.cz> [Accessed 20 September 2018].
- [50] Proposal for a directive of the European parliament and of the Council on the re-use of public sector information (recast). COM/2018/234 final – 2018/0111 (COD). 25 April 2018. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information> [Accessed 11 September 2018].
- [51] Proposal for a revision of the Directive 2003/98/EC on the reuse of public sector information. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/proposal-revision-directive-200398ec-reuse-public-sector-information> [Accessed 11 September 2018].
- [52] 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). *Official Journal of the European Union* (2016/L119/1). 4 May 2016. [online] Available from: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1520438094012&uri=CELEX:32016R0679> [Accessed 3 March 2018].
- [53] *Regulation of Ministry of Finance of the Slovak Republic No. 55/2014 Coll., On standards for public administration information systems*. Slovakia. In Slovak.
- [54] *Rpvs.gov.sk*. [online] Available from: <https://rpvs.gov.sk/rpvs> [Accessed 20 September 2018].
- [55] *Slov-lex.sk*. [online] Available from: <https://www.slov-lex.sk/domov> [Accessed 20 September 2018].
- [56] *Statement of reasons of the act that amended Czech Freedom of Information Act*. [online] Available from: <https://www.psp.cz/sqw/text/orig2.sqw?idd=112562> [Accessed 9 March 2018].
- [57] Study to support the review of Directive 2003/98/EC on the re-use of public sector information, pp. 134–140. [online] Available from: <https://publications.europa.eu/en/pu>

blication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en
[Accessed 11 September 2018].

- [58] *Ten Principles For Opening Up Government Information*. Sunlight Foundation. [online] Available from: <http://sunlightfoundation.com/policy/documents/ten-open-data-principles/> [Accessed 20 September 2018].
- [59] *The Open Data Handbook*. [online] Available from: <http://opendatahandbook.org/> [Accessed 20 September 2018].
- [60] Verhulst, S., & Young, A. (2016). *Open Data impact, when demand and supply meet. Key finding of the open data Impact case studies*. Opgehaald van. thegovlab.org. [online] Available from: <http://odimpact.org/key-findings.html> [Accessed 20 September 2018].
- [61] *Wypych v. Poland*. (2005) No. 2428/05, ECHR (Admissability decision).