Dopad obecného nařízení o ochraně osobních údajů na šedou literaturu

Koščík, Michal
2016

Dostupný z http://www.nusl.cz/ntk/nusl-261188

9th Conference on Grey Literature and Repositories: proceedings [online]. Prague: National Library of Technology, 2016 [cit. 2015-12-5]. Available from: **http://nrgl.techlib.cz/conference/conference-proceedings/**. ISSN 2336-5021.

THE IMPACT OF GENERAL DATA PROTECTION REGULATION ON THE GREY LITERATURE

Michal Koščík

koscik@med.muni.cz

Masaryk University, Czech Republic

Abstract

On 27 April 2016, the European Commission adopted new "general data protection regulation" that will be effective in all Member States from 25 May 2018. This article focuses on the impact of such regulation on the operators of grey literature, especially with regard to the administrative requirements introduced by new "privacy by design rules". The article also assesses the statutory licenses of a public repository to process and make available personal information even without the consent of a data subject.

Keywords

Data Protection, Privacy, GDPR, GDPR Compliance

Introduction

Compliance with data protection rules and the privacy awareness of the operators of grey literature repositories have gradually improved over the past decade. Operators in the Central European region have invested significant amounts of time, resources and effort to achieve

compliance and train their employees in data protection issues. They have also been adapting in recent years to developments in Case-Law of the European Court of Justice (hereinafter "CJEU") in order to comply with the newly-formulated right to be forgotten.

On 27 April 2016, the European Commission adopted new "general data protection regulation [1] " (hereinafter “GDPR”). In contrast to the previous data protection directive (95/46/EC), the regulation does not have to be transposed into the legal systems of individual Member States. The rules contained in GDPR have direct effect and will be effective in all Member States from 25 May 2018. GDPR is a rather extensive piece of legislation. Its recital has 173 points, the normative part has 99 Articles and the whole directive altogether takes up 88 pages of the official European Journal. Moreover, it is accompanied by the directive 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, which was adopted on the same day.

This article outlines the impact of new data protection rules on grey repositories and assesses the steps that need to be taken in advance to be prepared for compliance with the new regulation.

Continuity with the principles of the current directive

The adoption of GDPR was not brought about by any need to significantly change the fundamental principles of existing data protection rules, but rather by an acknowledgement that data processing technologies have changed significantly since the adoption of the current directive in 1995. As the recitals of GDPR state, the objectives and principles of Directive 95/46/EC remain sound (see recital 9. GDPR), but the legislation needs to address current conditions such as Rapid technological developments and globalization (see recital 6 GDPR), cross-border flows of personal data (recital 5 GDPR) and significant risks to the protection of natural persons, in particular with regard to online activity.

The definition of personal data remains extremely broad[2], as does the definition of personal data processing[3]. Basically every systematic work with any kind of information that contains references to individuals falls under the scope of GDPR unless it is done in the course of purely personal or household activity (Art. 2(2) GDPR) or by authorities responsible for forensic and security tasks.

GDPR preserves the concept of distinction between the “controller of data”, i.e. the person who determines the purpose of data processing, and the “processor of data”, who performs certain activities at the controller’s request. The **purpose** of data processing remains the central concept and starting point for any further considerations. Once the purpose has been defined, the controller and processor have to process data in accordance with fundamental principles

[1] 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); OJ L 119, 4.5.2016, p. 1–88.

[2] ‘Personal data’ means any information relating to an identified or identifiable natural person.

[3] "Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data.

of lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality[4]. It should be noted, however, that these concepts are also in line with the current data protection directive and case-law at the Court of Justice (CJEU). **The change is more a matter of more precise formulation of these principles than any fundamental change in basic concepts**. The exact formulation of the rules arising from these principles is more detailed and offers explicit solutions for cases which have been open to interpretation until now.

The principle of storage limitation and exception for archiving in the public interest

The principle of storage limitation is of great relevance to grey repositories. GDPR states that personal data must not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed (Art. 5(1)(e) GDPR). This means that the stored documents must be made anonymous at a certain point in time. GDPR, however, allows one major exception, i.e. long term processing "solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes". Hence, public repositories are generally entitled to collect, process, store and make available certain personal data, even if that information was not originally created or collected for the purposes of archiving in a repository.

The exception is not without restrictions. The use of every exception has to be balanced with the rights of the data subject. Learning how to balance public interest and the rights of an individual is the most important and most difficult legal question for any public repository.

Data protection by design and default – liability begins even before processing takes place

The concept of data protection by design is a certain form of good practice on the part of the data controller to design its processes and systems in order to minimize the risks of data protection breaches. GDPR introduces the obligation of the controller to take appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with GDPR (Art. 24). The controller is explicitly required to assess the risks and make plans for the security of data, both at the time of determining the means of processing and at the time of processing itself (Art. 25(1) GDPR)[5]. We believe that an explicit formulation of "privacy of design" principles will have little real impact since these principles are applied by most repositories even now. The obligation to be able to demonstrate such compliance at any point in time will, however, increase the paperwork and legal costs at every institution that stores and processes virtually any kind of documents. The paperwork that needs

[4] These concepts are explained in detail in Articles 5-11 GDPR.

[5] For further reference see Allen & Overy. *The EU General Data Protection Regulation - A new data protection landscape* [online]. 2016 [cit. 1.20.2016]. Available from: **http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf**.

to be done before, during and after processing and the records that have to be kept are defined in extensor to Article 30 GDPR. Fortunately, this extensive list is not applicable to institutions that employ less than 250 employees.

Processing data with and without consent

The processing of personal data is lawful if the person has given consent[6] to process his or her personal data. All consent must be “specific, informed and unambiguous" (Art. 4(11) GDPR) and has to be “made by a statement or by a clear affirmative action”. GDPR hence rules out the possibility of so called “opt-out consents”, i.e. schemes where a repository makes the individual aware that his data are collected and processed and presumes his consent unless the individual indicates otherwise. Hence, the request for consent must be given in an intelligible and easily accessible form and using clear and plain language and it must be as easy to withdraw consent as it is to give it[7].

Art. 6 GDPR sets forth five explicit exemptions when the controller may process documents with personal data without the consent of the data subjects. The operators of repositories will rely mainly on the exemption of “compliance with a legal obligation of a controller” (where certain documents have to be archived by law), "performance of tasks in the public interest" (especially repositories operated by public libraries) or "other legitimate interests pursued by the controller", providing that such interests are not such interests that are "overridden by the interests or fundamental rights and freedoms of the data subject".

GDPR does not specify which purposes are legitimate in justifying processing without consent and which are not. However, the recitals of the directive set forth that it should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject. We can conclude by reading these provisions together with the exception to the principle of storage limitation in Art. 5 (see above) that public repositories which gather and process grey literature for archiving, scientific, historical research or statistical purposes do not necessarily require consent from any individual mentioned in the documents being processed. This does not mean, however, that their statutory license is not unrestricted. Operators will have to bear in mind the purpose of every single activity performed with a document that contains personal data.

Each activity and process that involves the document would have to be assessed in light of whether such activity is truly necessary for the public purpose. For example, if the repository concludes that archiving certain documents is within the public interest, it has to then ask whether posting such documents online is also within the public interest.

[6] It is widely discussed whether processing based on consent is the most appropriate way to approach data processing, see, e.g., MÍŠEK, Jakub. Consent to Personal Data Processing – The Panacea or The Dead End? *Masaryk University Journal of Law and Technology*. **8**(1), 69-83. ISSN 1802-5943.

[7] See EU GDPR Portal - **http://www.eugdpr.org/key-changes.html**.

Right to object and right to erasure (right to be forgotten)

A data subject has the specific right to object (see Art. 21 GDPR) to any form of processing of his/her personal data, even if the repository (as a data controller or processor) is a public institution which processes such data to fulfil its statutory tasks. The repository must invariably prove that the interest in processing such information overrides the interests or the fundamental rights and freedoms of the data subject.

Apart from the right to object, GDPR introduces special rules about information that is not only processed, but published as well. Grey repositories already have already had to adapt their policies to comply with the "right to be forgotten" rule which was formulated by the Court of Justice of the European Union in the "Google Spain"[8] case[9] from 2013. GDPR follows the ideological path outlined by the court in the Google Spain case and makes the lives of repositories marginally easier by providing clearer and explicit rules in a piece of legislation. The rules on "the right to be forgotten" or "the right to erasure" (these two terms have to be read as synonyms) are found in Art. 17. If the repository archives and/or publishes a document which contains personal data, the individual concerned can demand that these data be erased if such data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. These rules are in line with the Google Spain ruling. However, a new rule that goes much further to protect the interests of the data subject is introduced in Art. 17(2). A controller who has granted the right of erasure and erased personal information is obliged to inform other controllers that are processing such personal data to erase any links to, or copies or replications of, those personal data. In other words, if a repository publishes a copy of a document from a third party, it has to inform such party that a request to erase personal data has been made.

GDPR also articulates exceptions where a repository can justify the processing of personal data even against the request of a data subject to erase such information. The repository is entitled to keep its documents intact (even published) if the processing serves a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[10].

Anonymization, pseudonymization and profiling

The anonymization or pseudonymization of a document is a technique which is broadly used to manage risks of privacy or data protection claims. GDPR acknowledges these techniques as legitimate and states that anonymized data fall outside the scope of data protection regulation.

However, GDPR distinguishes between anonymized and pseudonymized information, which is any information that can be de-cyphered, whereby the individual can be tracked and

[8] Case C-131/12, ECLI:EU:C:2014:317

[9] A detailed analysis was published in 2014: KOŠČÍK, Michal. Privacy and anonymization in repositories of grey literature. *The Grey Journal. 2015*, **11**, 47-51. ISSN 1574-1796. MÍŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie*. 2015, (1-2), 30-34. ISSN 1210-6348.

[10] See recital 65 GDPR – the exact rules are formulated in the Art. 17(3) GDPR.

identified (even if the key to decipher pseudonyms is not in the possession of the entity that processes pseudonymized data). Hence, pseudonymized data are personal data and fall within the scope of the regulation. Pseudonymization is acknowledged as a technique that can reduce the risks to the data subjects concerned and help controllers and processors meet their data-protection obligations" (see recital 28 GDPR); it is emphasized, however, that pseudonymization cannot be the only technique deployed by the repository in order to comply with data protection rules.

Conclusion

It can be concluded that a repository operator that has taken data protection and privacy issues seriously will not have many problems in complying with the standards of GDPR. The positive side of GDPR is that it extensively formulates rules that have been open to interpretation by doctrine and the case law of European courts. It can be said that the European Commission does not stray from the widely accepted interpretations of the current Data Protection Directive, a fact which adds to the legal certainty of both data subjects and data controllers alike. Therefore, the main change, and main negative impact, of the directive is the increased requirements on paperwork and record-keeping, especially for institutions that employ more than 250 employees.

References

ALLEN & OVERY. *The EU General Data Protection Regulation - A new data protection landscape* [online]. 2016, [cit. 1.20.2016]. Available from: **http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf**.

KOŠČÍK, Michal. Privacy and anonymization in repositories of grey literature. *The Grey Journal*. 2015, **11**, p. 47-51. ISSN 1574-1796.

MÍŠEK, Jakub. Consent to personal data processing – The Panacea or The dead end? *Masaryk University Journal of Law and Technology.* 2014, **8**(1), p. 69-83. ISSN 1802-5943.

MÍŠEK, Jakub a Jakub HARAŠTA. Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie.* 2015, 1-2, 30-34. ISSN 1210-6348.

POLČÁK, Radim. Getting European data protection off the ground. *International Data Privacy Law.* 2014, **4**(4), 282-289. DOI 10.1093/idpl/ipu019.

SCHAAR, Peter. Privacy by design. *Identity in the Information Society.* 2010, **3**(2), 267-274. DOI **10.1007/s12394-010-0055-x**.