Well-being in Information Society 2014

Conference proceedings

Well-being in Information Society 2014
Conference proceedings

13-14 November 2014
University of Pécs

Editors:
Gábor Rappai - Csilla Filó

Layout and Cover Design:
z_

This is an open access book.

ISBN:
This book is available from
http://jollet.pii.pte.hu/menu/32/27

published by:
University of Pécs

supported by:
TÁMOP-4.2.2.C-11/1/KONV-2012-0005
European Union
European Social Fund

Content

New principles and instruments in the field of Data Protection Law

Kiss, A - Szőke, G. L.
National University of Public Service, University of Pécs (Hungary)

Background

The birth of data protection regulation in Europe was directly linked to technological developments – mainly to the impressive IT developments of the '70s and their application in public administration. These changes have challenged data protection law on every single day ever since.[54] One of the most important objectives of the data protection regulation is decreasing the information power of data controllers by providing limitations on processing of personal data and limitations of combining different databases.

Data protection Acts of the 70s, sometimes referred to as the first generation of data protection regulation, were enacted in a world where few data controllers (mostly government bodies and some major companies) used automated data processing technology, and where the general purpose was to limit the state's power by ensuring the transparency of the state's databases.[55]

In the 80s and 90s the world changed a lot – also from privacy risks' perspective. Various developments such as the spread of personal computers (PCs) and the wide usage of it by business sector imposed potential new risks. Later, from the middle of the 90s, the rapid expansion of Internet usage and the appearance of many online services set new challenges for regulators. The establishment of the "information society" became a political agenda in the European Union, and so documents were adopted in this field, all emphasizing the importance of privacy.[56] The legal regulation of personal data changed a lot in the 90's in order to face these challenges. The main result was the adoption of the European Data Protection Directive.[57]

During the last 10-15 years, there have been further significant social, economic and cultural changes which EU legislation has had to face and respond to, like web 2.0, cloud computing, ubiquitous computing, mobile data processing, new ways of profiling and Big Data.[58]

[54] Kiss – Szőke, 2015, 311-312.
[55] Jóri, 2005, 24-25.
[56] Kiss – Szőke, 2015, 314-315.
[57] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[58] Kiss – Szőke, 2015, 316-317.

Besides these tendencies, the all-encompassing digital governance and surveillance methods grant for the state a ubiquitous monitoring option and a valuable database containing a wide range of personal data. In addition to the basic services, like online enrolment in higher education or filling in tax return, electronic government includes the use of interconnected databases, biometric identification systems (e.g. to issue personal documents), tracking systems such as RFID tags and geographical positioning systems, camera surveillance, and the collection of vast amounts of citizens' data through everyday transactions. These make governments one of the largest data processors (together with multinational companies) of the 21st century. On the other hand they have to face concern among citizens about the possibility of intrusive data collection, misuse or loss of personal information, and constant surveillance practices, just to mention some of the top barriers in the progress of electronic governance.[59]

European data protection reform

The legal framework currently in force in the EU Member States cannot provide adequate answers to the problems of mass data collection by the state and by companies, and the lack of transparency and efficiency in their processing activities, while the development of applicable information security (and identity management) is an ongoing challenge.[60]

Currently, the European data protection law is undergoing a long awaited revision. One of the most important aims of the reform is to react appropriately to the latest technological developments (like Big Data) and to the related social changes once more.

In our research, we have investigated, whether the development of data protection will be or could be able to face the challenges of the mentioned technological changes or not. As for the key outcome, it seems that a new philosophical approach is needed in the regulation. The core element of this should aim at the effective protection of individual privacy, even if subjects' privacy awareness is low, or no steps are taken by them in order to be protected. In other words, there is an elementary need for ensuring a form of »background protection«. Therefore our research team has analyzed the key elements of the Proposal for a new European Data Protection Regulation[61] in details, to decide whether it could fit into this new approach. We have concluded, that the Proposal for the GDPR is more relevant than a simple fine-tuning of existing legislation and the focus is clearly shifting to the issues of »what the data controllers shall do«, from the question of »what the data subject has the right to«."[62]

[59] Jacobi et. al., 2013, 14.
[60] Kiss, 2014, 267.
[61] European Parliament, "European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR)" (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212 [30.06.2014.]
[62] Kiss – Szőke, 2015, 329.

Law and Technology

Theories of Lawrence Lessig argue that the Code (that means both regulation and computer program lines) has a major relevance in cyberspace. This Code, which includes software, hardware, and the entire online infrastructure, as a general rule defines cyberspace, innovations and also the permitted and forbidden behaviours.[63] However, European data controllers are obliged to process personal data in line with not just the Code, but all principles of the EU Directive on data protection and will have to face a number of new duties under the framework of GDPR.[64] Therefore the use of technologies and principles which foster the legitimate processing of data could effectively reduce the costs of meeting the obligations and the chance of being sanctioned for illegal data processing activities.[65]
For that reason, the second main goal of our research was to sum up how technological developments change the regulation of personal data processing, and what are the new principles of the GDPR that aims to regulate the issue of privacy invasive technologies and projects. The principles of Privacy by Design and Privacy by Default, including one of their key instruments, Privacy Enhancing Technologies (PETs) were the subjects of many scientific research papers of the team.

Article 23 of the GDPR impose the principle of Privacy by Design (PbD) stating that „Where required, mandatory measures may be adopted to ensure that categories of goods or services are designed and have default settings meeting the requirements of this Regulation relating to the protection of individuals with regard to the processing of personal data." PbD is the new corporate hotness affecting IT systems, business practices, and networked infrastructure.[66] It is the concept of embedding privacy into the design specification of various technologies, and also a set of rules laying down ideas of taking a proactive approach contrary to the Surveillance by Design phenomenon, appearing in the US in the 90's.[67] Although PbD was evolved originally in the technology area, its scope expanded to business practices and physical design due to the works of Ann Cavoukian.[68] This approach is applicable for all types of data processing, especially for processing sensitive data, such as health or financial data, and includes the determination of the means for data processing and at the time of the processing itself.

The meaning of Privacy by Default is similar to PbD, however needs even more attention on the data controllers' side – to protect privacy in cases when there are multiple choices to select the level of protection, but the user remains passive. In this case the default setting shall provide the highest level of protection (e.g. Do Not Track settings in Internet browsers).

[63] Lessig, 2006, 5.
[64] Balogh et al., 2014a,
[65] Rubinstein, 2012, 1411.
[66] Hill, 2011.
[67] Böröcz, 2014a, 280-281.
[68] Cf. Cavoukian, 2009.

Privacy Enhancing Technologies refer to a "system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."[69] It is more than just a field of research in IT security, as the key goal is to enforce legal privacy principles.[70]

Although there is an overlap in the aims of PbD and PETs, the latter are clearly engineering approaches which focus on the positive potential of technology, on tools used to maintain anonymity, confidentiality, or control over personal information,[71] whilst PbD is a broader concept comprising several elements[72] to balance technologies with a framework highlighting the process and their fundamental components.[73]

On one hand side, in various projects, where the processing of personal data is necessary and have a legitimate purpose, the introduction of PETs can serve as a technological and institutional background to enforce the principle of data minimization, both at communicational and at application level (e.g. by providing anonymous communication, securing online transactions). On the other hand, some PETs are also tools for the creation and analysis of machine readable privacy policies, therefore enhancing transparency and legitimacy in data processing, facilitating users to exercise their right of informational self-determination.[74] PETs can be deployed at both ends, by controllers and data subjects, therefore with the combination of these solutions privacy enhancing identity management can be introduced for users and data controllers, tools that allow users to negotiate privacy policies with service providers.[75] However, PETs have to be developed directly to face the challenges of the invasive technologies' development, and to be more understandable for the everyday user.[76]

Data security, in close relation to privacy, is a crucial issue of data processing. A series of legal, organizational, and technical safeguards, appropriate to the sensitivity of the information are needed in order to ensure that data maintained are remaining confidential, integral and available only to authorized persons. Laws governing authorization, encryption of data and procedures to protect files are enacted differently in the EU Member States, implementing the general rules of Article 16 and 17 of the Directive, while there is a lack of cooperation between IT specialist and policy makers. The level of data security can be enhanced either by introducing obligatory compliance of data controllers to standards (such as ISO or Cobit),[77] or by the application of new

[69] van Blarkom – Borking – Olk, 2003, 33.
[70] „Data security technologies are PETs if they are used to enhance privacy. But, it should be noted that they can be used in inherently privacy-invasive application, in which case they cannot properly be counted as PETs." London Economics, 2010, ix.
[71] Rubinstein, 2012, 1412.
[72] Cf. Cavoukian, 2011.
[73] Rost – Bock, 2011, 1.
[74] Kolter, 2009, 31.
[75] Leenes – Schallaböck – Hansen, 2008, 17.
[76] Kolter, 2009, 2.
[77] Szádeczky, 2013, 153.

PETs, that also increase the level of protection of personal information by setting the protection of personal data as 'default' in different services, as a result making the use of technology one of the key elements of a suggested new European legislation.[78]

The Article 30 (1) of the GDPR also imposes the obligation on data controllers to take security measures in accordance with "taking into account the results of a data protection impact assessment". Contrary to the current regulation, data controllers and processors should adopt (written) security policies to comply with the new provisions of Article 30 (1a) of the GDPR.

Data Protection Impact Assessment

One of the most important novelties of the future data protection law is data protection impact assessment. First of all, the GDPR lays down for all data controllers the obligation to carry out a risk analysis of the potential impact of the intended data processing. If specific risks are likely to be presented by the data processing, the controllers shall also carry out data protection impact assessment and periodical compliance review. The Proposal lists the circumstances of data processing operations which are likely to present specific risks; e.g. processing of more than 5,000 data subjects' personal data, or processing special categories of personal data (sensitive data), or profiling, if it has legal effects on data subjects, automated monitoring of publicly accessible areas on a large scale (like CCTV systems), etc. For that reason the obligation to carry out data protection impact assessment concerns a well-defined, but somewhat wide range of data controllers.[79]

Carrying out a Privacy Impact Assessment is far not an easy task to do. In order to help out the data controllers in our research, we summarized the most important element of a PIA methodology,[80] based on the newest European tendencies and research results,[81] and on actually working best practices of the US, Canada and Australia. In these countries privacy impact assessment is mostly used for the data processing operations of the public sector's body and of the health care system.[82]

Generally it can be said, that a "privacy impact assessment (PIA) is a process for assessing the impacts on privacy of a project, policy, program, service, product, or other initiative (hereinafter: project) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize the negative impacts. The concept of PIA has been known since the mid '90s and has become progressively more common. The growing interest in PIA is caused by the robust development of privacy-invasive tools."[83]

[78] Kiss, 2013, 116.
[79] Kiss – Szőke, 2015, 321.
[80] Balogh – Böröcz – Kiss – Polyák – Szőke, 2014
[81] De Hert – Kloza, – Wright, 2012
[82] Böröcz, 2014b, 104.
[83] De Hert – Kloza – Wright, 2012, 5.

The main important elements of a PIA process are:

- Deciding whether PIA is necessary at all;
- Choosing the organization who carries out the privacy impact assessment;
- Project description;
- Pointing out potential privacy implications;
- Consultation with the stakeholders;
- Risk management (including assessment and mitigation);
- Legal compliance check;
- Drawing up recommendations;
- Reporting;
- Implementation of recommendations (including the justification of the non-implemented recommendations);
- (Periodical) compliance review [84]

In our research the characteristics and key elements of all of these steps have been summarized, taking into account the planned provisions of the GDPR. As a result of the project a detailed questionnaire with 29 exact questions have been worked out, which may be applied in various PIA processes. Thus, these results are widely applicable for data processing activities of data controllers.

Summary

Our research in the past two years has focused on the new tendencies and new legal institutions in the field of data protection law. We have analyzed the European data protection reform, including the most important output of this process, the Proposal for new Data Protection Regulation. We have concluded, that the Proposal for the is more relevant than a simple fine-tuning of existing legislation and the focus is clearly shifting from the rights of data subjects to the compliance duties of the data controllers. We have also shown the increasing role of the technology as a regulatory means, and the emerging of a new principle calls "Privacy by Design". "Setting strict rules for data controllers on applying technologies for personal data processing fits the concept of a paradigm shift; it can be seen as a change in balancing responsibilities from the data subjects' informational self-determination towards an automatic protection."[85] Finally we've put the focus of the research activity on the new legal instrument of "privacy impact assessment", and have summarized the most important steps to carry out such process. These results are widely applicable for data processing activities of data controllers and offer an actual help for them to increase the level of data protection, which totally fits to our original research goals.

[84] Balogh – Böröcz – Kiss – Polyák – Szőke, 2014, 80., De Hert – Kloza – Wright, 2012, 27-32.
[85] Kiss-Szőke, 2015, 12.

References

Balogh Zsolt György – Kiss Attila – Polyák Gábor – Szádeczky Tamás – Szőke Gergely László (2014a): Technológia a jog szolgálatában? Kísérletek az adatvédelem területén. Pro Futuro - A Jövő Nemzedékek Joga 4 (1), pp. 33-46.
Balogh Zsolt György – Böröcz István – Kiss Attila – Polyák Gábor − Szőke Gergely László (2014b): Az adatvédelmi hatásvizsgálat módszertana, Médiakutató, 2014/4, pp. 77-92.
Böröcz István (2014a): The tools of privacy protection at the dawn of a new era. Privacy by Design in theory and in practice. In: Alexander Balthasar, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Johannes Pichler (eds.): Central and Eastern European eGov Days 2014 - eGovernment: Driver or Stumbling Block for European Integration. Austrian Computer Society, Wien, pp. 269-282.
Böröcz István (2014b): A Privacy Impact Assessment forrásai, *Infokommunikáció és jog 59,* 2014/3, pp. 103-110.
Cavoukian, Ann (2009): Privacy by Design. …Take the challenge. Information and Privacy Commissioner of Ontario, available at: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [13/11/2014]
Cavoukian, Ann (2011), "Privacy by Design, The 7 Foundational Principles," available at: http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf [13/11/2014]
De Hert, Paul – Kloza, Dariusz – Wright, David (2012): Recommendations for a privacy impact assessment framework for the European Union. http://piafproject.eu/ref/PIAF_D3_final.pdf [2013.07.17.]
Hill, Kashmir: Why 'Privacy by Design' is the New Corporate Hotness, 2011, Available at: http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/ [13/11/2014]
Jacobi, Anders. – Jensen, Mikkel Lund – Kool, Linda – Munnichs, Geert – Weber, Arnd (2013): Security of eGovernment Systems, Science and Technology Options Assessment, European Union, Brussels, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/513510/IPOL-JOIN_ET%282013%29513510_EN.pdf [31.01.2014]
Jóri, András (2005): Adatvédelmi kézikönyv, Osiris, Budapest.
Kiss Attila (2013): A privátszférát erősítő technológiák, *Infokommunikáció és jog 56*, 2013/3, pp. 113-120.
Kiss, Attila (2014): The European data protection legal framework in relation to e-Government. In: Alexander Balthasar, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Johannes Pichler (eds.): Central and Eastern European eGov Days 2014 - eGovernment: Driver or Stumbling Block for European Integration. Austrian Computer Society, Wien, pp. 253-268.
Kiss, Attila – Szőke, Gergely László (2015): Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation, In: Gutwirth – Leenes – De Hert (eds.): Reforming European Data Protection Law, Springer, pp. 311-332.

Kolter, Jan P. (2009): User-Centric Privacy. A Usable and Provider-Independent Privacy Infrastructure. Dissertation, University of Regensburg, available at: http://www.ics.uci.edu/~kobsa/phds/kolter.pdf [13/11/2014]
Leenes, Ronald - Schallaböck, Jan - Hansen, Marit (2008): PRIME white paper. Third and final version, available at: https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf [13/11/2014]
Lessig, Lawrence (2006): Code, Version 2.0, Basic Books, New York. http://codev2.cc/download+remix/Lessig-Codev2.pdf [13/11/2014]
London Economics (2010): Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [13/11/2014]
Rost, Martin – Bock, Kirsten (2011): "Privacy by Design and the New Protection Goals," available at: https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf [13/11/2014]
Rubinstein, Ira S. (2012): "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26, pp. 1410–1456.
Szádeczky, Tamás (2013): Az IT biztonság szabályozásának konfliktusa, *Infokommunikáció és jog 56*, 2013/3, pp. 151-155.
Van Blarkom, G. W. − Borking, J. J. − Olk, J. G. E. (eds.)(2003): Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents. College bescherming persoonsgegevens, The Hague.