An Impact of General Data Protection Regulation on a Smart City Concept

Dražen Lučić*, Marija Boban**, Danijel Mileta***
* Zagreb, Croatia,
** Faculty of Law, University of Split, Split, Croatia
***Polytechnic of Šibenik, Šibenik, Croatia
drazen.marko.lucic@gmail.com
marija.boban@pravo.st
danijel,mileta@gmail.com

***Abstract* - The paper deals with a possible impact of implementation of General Data Protection Regulation on a Smart City concept in the area of electronic communications. The stake holders at electronic communications market will need to ensure full compliance with the General Data Protection Regulation, ePrivacy regulation and the directive on security of network and information systems. Rigid application of data protection and e-privacy rules may slow down or even jeopardize roll out of the solutions for both Internet of Things and a Smart City concept. The roles of national regulatory authorities have been described in the case of Republic of Croatia.**

Keywords – General Dana Protection Regulation, Smart City, electronic communications market regulation, Internet of Things, National Regulatory Authority

I. INTRODUCTION

Last years European commission has been working on several documents that will strongly influence data processing business. In April 2016 EU Parliament introduced General Data Protection Regulation (GDPR) [1]. In EU internet page is described that "GDPR was designed to harmonize data privacy laws across Europe, to protect and empower EU citizen data privacy and to reshape the way organizations across the region approach data privacy".

GDPR is a data protection law which is going to come in force on 25th of May, 2018 [2]. This regulation applies to any organisation that controls or processes the data of an EU resident. The regulation has a significant impact on business in all industry sectors, bringing changes for business in terms of both cost and effort. The introduction of new rights for individuals, such as Right to be Forgotten and the Right to Portability, as well as introduction of mandatory breach notification, are likely to increase the regulatory burden for both companies and governmental institutions. They need to review their current data protection compliance programs in order to determine next steps and furthermore decide on the level of investment they need to make, so as to address the change. On the same day e-Privacy regulation aligned with GDPR rules will be enforced as well. Therefore, in a single month, companies will need to ensure they have everything necessary in place to comply with the new GDPR, e-Privacy regulation [3] and the Directive on security of network and information systems ("NIS Directive") [4]. This has also a huge impact on electronic communications market regulation in EU with influence on EU single digital market and EU Digital agenda 2020 [5].

In parallel there is an another interesting process ongoing. The global societal challenges related to health, ageing and wellbeing, energy, transport and environment, inclusive, innovative, reflective and secure societies are and will be expressed particularly in the city. Smart systems connecting physical world and information world and providing autonomous mode of operation are recognized as part of the solution. Particularly important is the role of the Internet of Things (IoT) [6 - 9]. Smart City is a concept of urban development that comprises economic, social and environmental aspects of a city and quality of life of citizens. Basic technology behind such a complex development is Information and Communication Technology (ICT) enabling interaction and collaboration among citizens, services related to city physical and social infrastructure offered to them, and implementation and operation of smart systems for a smart city. International Telecommunication Union (ITU), among some other organisations, has established Study Group on Internet of things and smart cities and communities working on ITU-T Recommendation series Y. 4000 [10 - 14].

In this paper possible impact on electronic communications markets regulation in EU by implementation of GDPR, together with "ePrivacy regulation" and "NIS Directive", has been elaborated. General influence of GDPR omnibus data protection laws on electronic communications market regulation has been outlined in the second section of the paper. An impact of GDPR on a Smart City concept is described in the third section. The role of a national regulatory authority (NRA) for electronic communications in EU is discussed in the section four in the case of Croatian NRA, Croatian Regulatory Authority for Network Industries (HAKOM).

II. POSSIBLE IMPACT OF GDPR ON ELECTRONIC COMMUNICATIONS MARKETS IN EU

The transformation to digital society and digital economy is one of the results of ongoing process of digitalisation and globalisation. The creation of digital single market in EU has provoked that digital economy in EU has become increasingly reliant on the control and processing of personal data. On one side this process creates enormous opportunities for business but on another side could become obstacle or even a huge hurdle in implementation of new technologies. The process is accompanied by a growing public awareness and concern for the importance of personal data protection. The EU's response to this concern is GDPR:

Personal data protection is one of the key issues to be addressed by telecommunications network operators, given the importance of transparency and the risk of personal data breaches. Personal data management and protection gains a high attention especially by large operators which processes a large data volume about their end-users and end-users services. The implementation of GDPR and full compliance to GDPR, ePrivacy and „NIS Directive" introduce numerous requirements regarding the confidentiality and security of personal data. This process implies also a number of changes that the operators will need to implement, particulary in terms of personal data processing and protection.

Each operator, as the first step, has to find out where they have personal data, as well as to identify all data flows, boith internal and external, i.e. in the own country, outsided own country but within EU and outside EU. The operators have to perform an assesment whether local data protection laws and regulatory obligations need to be considered. They have to identiy all possible data sources, not only digital ones but also paper ones, audio and video recording, pictures, archived documents, etc.

Keeping space with the evolving threat landscape is a challenge even without the GDPR's stipulation for defences of contemporary threats in ICT. The problem partly comes from the way cyber security has evolved because every new way of attack produces a need for a new security solution to be added. Although each such additional solution may fulfil its role as it has been intended to do, it does mostly with little or even no interaction with the rest of the security infrastructure. This is not only hard to manage but can easily lead to gaps and inconsistencies in the response to new threats. Especially across a multi-vendor environment. The challenge is compounded by the adoption of trends such as mobility, cloud computing and IoT, all of which expand the effective attack surface, exposing new vulnerability and eroding the traditional concept of a telecommunication network border.

One of possible responses to those new threats is to increase processing and control. Additional processing power also adds complexity, thus multiplying the number of data points to be aggregated and interpreted when evaluating the best response to any detected event. Any "state of the art" solution will not only need to overcome the above-mentioned challenges but continually adapt to changes in the usage of technology and evolving threat landscape. Independently which solution will be applied, total cost of ownership for network operator will be increased by full implementation of GDPR in order to fully and timely comply to the GDPR requirements. These costs could arise to a level that there is no positive business case for an operator to implement a new technical solution or an end-user service which is based on a new technology like IoT. Furthermore, an additional obstacle in implementation of new technology due to GDPR could be complexity of administrative procedures that should be undertaken by both operators and end-users in order to fully comply to GDPR requirements, as well as additional costs connected to these procedures.

III. AN IMPACT OF GDPR ON A SMART CITY CONCEPT

Electronic communications have gone through a completely different process, from state monopoly to a competitive market of electronic communications. This transition was governed by statutory regulation. The present situation in the EU is defined by the common regulatory framework for electronic communications [15]. According to a Framework Directive, the NRAs shall "contribute to the development of the internal market", "promote the interests of the citizens", and "promote competition in the provision of electronic communications networks, electronic communications services and associated facilities and services by *inter alia*: (a) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price, and quality; (b) ensuring that there is no distortion or restriction of competition in the electronic communications sector; (c) encouraging efficient investment in infrastructure, and promoting innovation; and (d) encouraging efficient use and ensuring the effective management of radio frequencies and numbering resources".

Different approaches have been applied to regulate certain issues in electronic communications, and regulatory objectives have changed in line with technological and market changes. The same process is needed in the future, but at a faster rate. The development of the information and communication technology including networks, services, applications and content is exceptional, as is the research and innovation in this area. This must also be reflected in the governance and regulation of electronic communications, including the Internet, in order to be able to adapt to changing environments and prepare solutions for evolved and predicted problems. Different types of problems require different regulation tools, i.e. different solutions for different circumstances. The need for smart regulations that are effective and solution-oriented, ranging from no-regulation (deregulation), self- and co-regulation, to statutory regulation, has been recognized [16]. Such a regulation space and its three dimensions is shown in Figure 1. These three dimensions are: type, impact and topic.

Changes are also expected in the manner in which regulation is implemented: from vertical solutions for a specific network or service towards solutions for multiple, in some cases all, networks or services. Many systems and services that combine features from different paradigms require such solutions, for instance using IoT for sensing and collecting data and cloud computing to store it and execute applications [17-19].

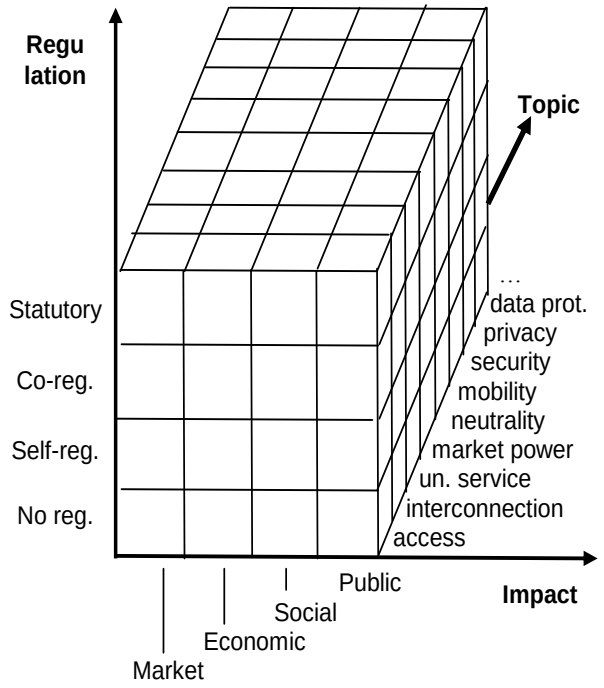

Figure 1. Market regulation space

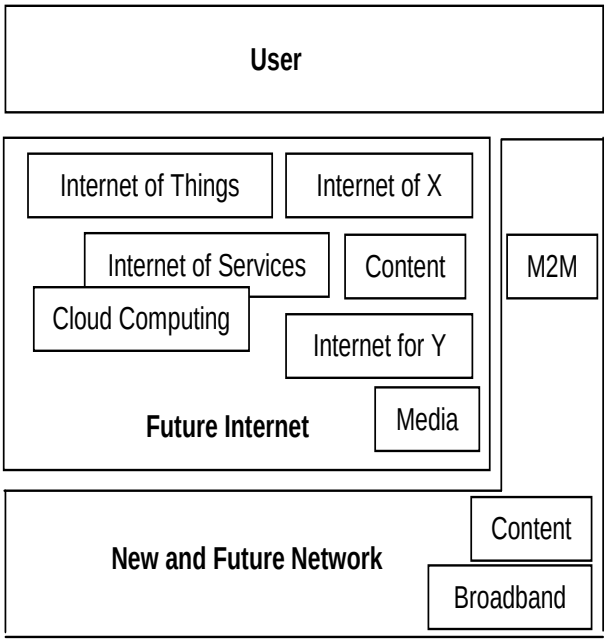

Figure 2. Future of Networking Landscape

Research and development of IoT solutions for Smart City is a global process but implementation is a local process that should take into account the specific issues and requirements of each city in order to produce benefits for its citizens and promote public interest. One of these specific local requirements is also data protection law and regulatory framework. The question is whether these regulatory directives will ensure trustworthiness or it will become a burden to the faster development of IoT, especially in the context of Smart City [20]. New GDPR and e-privacy directive features, like right to erasure, privacy by design and by default, data portability and data breaches rules will raise the level of trust in IoT technology for sure [21]. However, pseudonymisation as one of the major pillars of GDPR can have negative impact on further development [22]. New requirements relating to content- and service-awareness, computing capabilities, ubiquitous broadband access and mobility, massive connectivity of various devices and objects reflect on security, privacy and data protection. IoT, cloud computing as the enabler of Internet of Services (IoS), communication Machine-to-machine (M2M), and new paradigms related to content and media on the Internet are widely used, as it is shown in the Figure 2.

Transformation of personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information is very expensive process. IoT devices, like sensors or actuators, that collect such data, usually have limited processing power and are battery powered. Applying data protection and privacy rules on such devices may slow down or jeopardize roll out of IoT. Therefore it is necessary to take care of horizontal architecture of IoT when implementing these functionalities.

IV. The role of HAKOM as Croatian NRA

HAKOM, as Croatian NRA, together with academia in Croatia within the research project "Looking to the future 2020", work on creating an ecosystem open to the implementation of new communication technologies as IoT enablers. One of the goals of the project is to promote advantages and opportunities of IoT, thus encouraging and fostering the idea of human-centric digital age. The project members work, among other topics, on identification of the elements that may have an impact on the further development of IoT. While limited national resources, like radiofrequency spectrum, numbering and addressing will prove to be an issue in the future, lack of understanding and knowledge of security and privacy may slow down development already today. The role of HAKOM as the NRA for electronic communications is twofold, the market regulation in collaboration with other regulatory authorities and encouragement of the introduction of IoT.

Some policy and regulatory issues fall within the scope of electronic communications, but topics related to privacy, security protection require responsibility across the entire IoT value chain. National regulatory authorities for electronic communications having wide experience in all these areas can play significant role in development of trustworthy IoT for Smart City [23]. A close cooperation of HAKOM with national Private data protection agency, as well as with government and market stake holders, is essential prerequisite for a successful implementation of GDPR without jeopardising operators' business plan and time plan for implementation of new technical solutions and innovative end-user services, based on new technologies.

If there is no NRA for private data protection and/or there is no national act/law about private data protection, there is a concern about human rights and privacy of the citizens. Theoretical example of possible violations are numerous [24] while practical experience already confirms cases of privacy violation in applied Smart City concepts, not only outside Europe, but also in EU [25, 26].

V. CONCLUSION

A new approach to security, ePrivacy and data protection is required in order to fully and timely comply to GDPR requirements. The operators of electronic communications network have to connect together all key components of the security infrastructure in a seamless fabric thus enabling a successful implementation of the solutions and innovative end-user services, based on a new technologies. This process could be very expensive for an operator and can jeopardize their business plan an time plan for implementation of the solution that boost development of digital society, digital economy and single digital market in EU. Typical example is implementation of IoT as the base for a Smart City concept where administrative procedure and additional solution complexity due to obligatory compliance to GDPR requirements can not only significantly increase the cost of ownership but also turn the solution to high complexity and make it unattractive for end-users, or even unusable for them.

The role of the NRA for electronic communications is discussed from broader regulatory perspective involving public policy related to deployment of IoT and development of trustworthy IoT. This has to be done in close cooperation with national private date protection regulatory authority, government and market stake holders. An ultimate common goal is to boost digital economy by deployment and innovative end-user services which are based on new technologies and in the same time to fully comply to GDPR and to turn out GDPR requirements from obstacles and challenges into business opportunities.

ACKNOWLEDGEMENTS

The authors acknowledge the support of the research project “Looking to the Future 2020,” funded by Croatian Regulatory Authority for Network Industries (HAKOM).

REFERENCES

[1] „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)“, REGULATION (EU) 2016/679, 27 April 2016

[2] „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“, DIRECTIVE (EU) 2016/680, 27 April 2016

[3] “Regulation of the European Parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (regulation on Privacy and Electronic Communications)

[4] “The Directive on Security of network and information systems (NIS Directive)”

[5] „A Digital Agenda for Europe”, Communications from the Commission to the European Parliament, the Council, the EuropeanEconomic and Social Committee and the Committee of Regions, COM(2010) 245, Brussels, Belgium, 19.5.2010.

[6] I. Brown, „Regulation and the Internet of Things“, GSR Discussion Paper, 15th Global Symposium for. Regulators, ITU International Telecommunication Union, 2015.

[7] „Advancing the Internet of Things in Europe“, Commission Staff Working Document Accompanying the document Digitising European Industry Reaping the full benefits of a Digital Single Market COM(2016) 180 final, SWD(2016) 110 final, Brussels, 19.4.2016

[8] „Enabling the Internet of Things“, Report, BEREC – Body of European Regulators for Electronic Communications, BoR (16) 39, 12 February 2016.

[9] „ITU-T Study Group 20 - Internet of Things, smart cities and communities”

[10] „Draft Framework for Cyber-Physical Systems, Release 0.8“, CPS Public Working Group, National Institute of Standards and Technology, US Department of Commerce, September 2015.

[11] „Smart cities, Preliminary Report 2014“, ISO/IEC JTC 1, Information technology, 2015.

[12] „Shaping smarter and more sustainable cities - Striving for sustainable development goals”, ITU-T’s Technical Reports and Specifications, International Telecommunication Union, Geneva, Switzerland, 2016

[13] „Developing a Consensus Framework for Smart City Architectures - IIES-City Framework”, National Institute of Standards and Technology (NIST), 21 January 2017 (https://pages.nist.gov/smartcitiesarchitecture/)

[14] EpoSS – The European Technology Platform on Smart Systems Integration

[15] “Regulatory framework for electronic communications”

[16] D. Lucic, A. Caric and I. Lovrek, „Standardisation and Regulatory Context of Machine-to-Machine Communication”, Proceedings ConTEL 2015 13th International Conference on Telecommunications, Graz, Austria, 2015, pp. 1-7.

[17] D. Lucic, M. Weber and I. Lovrek, “Electronic Communications as Smart City Enablers”, Proceedings 2016 International Conference on Smart Systems and Technologies (SST), Osijek; Croatia, 2016, pp. 241 – 247

[18] M. Weber, D. Lucic and I. Lovrek, “Internet of Things Context of the Smart City”, *Proceedings 2017 International Conference on Smart Systems and Technologies (SST)*, Osijek; Croatia, 2017, pp. 187 - 195

[19] S. K. Datta, C. Bonnet, „Internet of Things and M2M Communications as Enablers of Smart City Initiatives”, Proceedings 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 2015, pp. 393-398.

[20] R. H. Weber, „Internet of Things – New Security and Privacy Challenges”, Computer Law and Security Review, 26(2010), 2010, pp. 23-30.

[21] K. Zhang, J. Ni, K. Yang, X. Liang, j. Ren, X Shen: ”Security and Privacy in Smart City Applications: Challenges and Solutions”, IEEE Communications Magazine, January 2017, pp 122- 129.

[22] N. Gumzej, „Protection of Data Relating to EU Consumers in the IoT Age”, Proceedings SoftCOM 2012 20th International Conference on Software, Telecommunications and Computer Networks, The 2nd Workshop on Regulatory Challenges in the Electronic Communications Market Split, Croatia, 2012, pp. 1-6

[23] „Summary report on the outcomes of the workshop on IoT technologies and their impact on regulation “, Report, BEREC – Body of European Regulators for Electronic Communications, BoR (17) 40, 24 February 2017

[24] A. AlDairi, L. Tawalbeh: “Cyber-Security Attacks on Smart Cities and Associated Mobile Technologies”, The International Workshop on Smart City Systems engineering” (SCE 2017), Procedia Compuetr Science 109C, 2017, pp. 1086 – 1091

[25] L. van Zoonen: “Privacy Concerns in Smart Cities”, Government Information Quarterly, No, 33, 2016, pp. 472 - 480

[26] S. Ijaz, M. Ali Shah, A Khan, M. Ahmed: "Smart Cities: A Survey on Security Concerns", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016, pp. 612 - 625