Will the GDPR slow down development of Smart Cities?

Goran Vojković, Ph.D.

University of Zagreb
Faculty of Transport and Traffic Sciences
Vukelićeva 4, Zagreb, Croatia
E-mail: goran.vojkovic@fpz.hr

Summary - After four (4) years of preparation and debate the General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14 April 2016. Enforcement date is 25 May 2018. The EU General Data Protection Regulation replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, but also to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. This Regulation is a legal act which is mandatory and fully valid for all EU Member States. Thereby, Member States may additionally regulate certain areas of personal data protection. Apart from being more appropriate for today's era of fast speed Internet and Internet of things (IOT), the new Regulation is essentially more extensive, more accurate, and involves the questions of personal data risk. Considering the fact that personal data is being processed in the E-business and E-government, and in addition to introduction of some smart-city functions, it's possible to indirectly collect personal data. The GDPR is extremely important and it's one of the key legal documents for the further development of the digital economy and administration. As this year's MIPRO almost coincides with the date of full implementation of the Regulation, it was an additional incentive to decide on a subject of invited lecture on GDPR.

Key words: personal data, GDPR, smart city

I. INTRODUCTION

With the GDPR's entry into force a legitimate question appeared; whether a new, and substantlly stricter form of personal data protection in Europe will limit the development of Smart Cities?

Although smart city deals with a citizen as a single or a group of citizens (e.g. in traffic), and with a smart city development system, personal data usually aren't important, they are collected simply by applying technology (e.g. video surveillance).

The new General Data Protection Regulation (GDPR) [1] begins to fully apply on 25 May 2018. This is a new act that regulates the matters of personal data protection in the EU countries in a very different way. Let us remember that the first modern act relating to this area is the Convention on the Protection of Individuals regarding the automatic processing of personal data [2] of the Council of Europe (Convention 108). This is the Convention of the Council of Europe, but since all EU members are also members of the Council of Europe, the Convention has been generally applied and applies within the EU.

The European Union has reformed the area of personal data protection in 1995 when the 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 [3] came into force. This Directive, together with Convention 108, is the foundation for the adoption of national personal data protection laws, the establishment of national regulatory agencies and the existing personal data protection model, which has been developed by so far.

Since the adoption of Directive 95/46/EC has passed many years, and it has begun to show some disadvantages, and legal practice has also shown that some standards can be regulated in a better manner. That is the reason why it all started with the adoption of a new regulation, and after a couple of years the GDPR was adopted.

This paper is written as a contribution to an invidited lecture for the International Convention MIPRO – for the section of Digital Economy and Government/Local Government/Public Services, and aims to show how new and accurate researches are needed in this area.

II. GDPR KEY CHANGES

As the GDPR has been and it still is written about, we are only listing the key changes in relation to the existing regulation, as the European Union itself states on specialized sites.

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. [4]

Data Subject Rights are: Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". Part of the expanded rights of

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 15,2025 at 01:37:26 UTC from IEEE Xplore. Restrictions apply.

data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where, and for what purpose. Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. Also, the Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing. Full list of new changes are assesible at cited page [4].

Preambule of GDPR has 173 paragraphs. Therefore, the GDPR has extensive and precise provisions, and for their non-compliance are foreseen vey high penalties, there is already a whole set of principles which should be respected in the process of application.

III. Smarty City

A common definition of a 'smart city' has not yet been determined. Many authors use various definitions to clarify what is a 'smart city'. Authors define it as a city that bets a lot on the quality of living and where the citizens are involved as main actors in decision processes [5].

However, one can find several identical links that have all the definitions. Cities have a duty to fulfill the needs of their citizens through various systems. The types of systems are by no means exhaustive, but certainly include public services such as light management, traffic and transport organisation, waste and water management, administration policies, security, energy sustainability and information services. Regular cities operate and supervise every system as a separate unit, which in return produces more costs for taxpayers with slight to no improvements in the quality of living. On the contrary, 'smart cities' use Information and Communications Technologies (ICT) with Internet of Things (further: IoT) to create connections and interactions between some or all of the systems, cutting expenses and improving the quality of life for citizens during the process. [6]

IV. Smarty City and GDPR are not always connected

Not all systems linked to Smart City will be directly related to basic data, especially those that are not of a high-tech nature. For example, carpooling; if we don't include applications for finding a driving partner, but only parking lots at the entrances of the cities, or next to the motorway entrances, then it won't have any relation to personal data.

It's similar to the systems which are not directly related to the people, for example data used for irrigation, or waste removal. The need for irrigation of the park is not directly dependent on the people who live there. There is a need to dispose of garbage cans (out of schedule), because the system detected an unpleasant smell, or are simply full - depends on people, but nevertheless in this example nobody collects one's personal data

However, there are activities where such division is not so simple. For example, a network of cycling trails; if not under video surveillance it has no connection with personal data, due to the fact that there is no personal data collection of natural persons who cycle on such trails. Still, if the city has a bicycle-sharing system (public bicycle system); one of the commercial models (e. g. Nexbike), or even its own, then when using city bikes; which is usually authorized and paid by credit cards; the personal data will inevitably be collected.

Let us also mention here how Smart City Models often use the IoT. And in that case, it's necessary to collect, access and dispose personal data appropriately. "Everyone acting in the IoT – no matter whether individual persons or business entities – must be able to decide for themselves what happens with the data they produce and for what purposes this may be done. The most important prerequisites for this are transparency and technical protection against misuse." [7]

V. Can Smart City represent danger for privacy?

Finally, we are asking the main question - will GDPR slow down the development of Smart City? The answer gives us the citation of several important parts of the Regulation.

In some cases, for example, microdemocracy (discussion and decision-making at the local level); there will be no larger scale problems - the respondents will give their own data with the consent if they like to participate in the discussions, and the controller must only precisely fulfill the tasks imposed by the GDPR. But what about systems where there are different levels of automation, and where a natural person does not report voluntarily?

According to the Art. 5. of the Regulation, personal data shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", also "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".

This clearly states that the collection of personal data for the purpose of developing Smart City must be precisely defined, with appropriate legal rules, and special attention should be paid to keeping the data; by which a natural person can be identified; which shouldn't be longer than it's necessary. Certainly, data can then be kept for statistical and other purposes, such as production of a traffic model, but they should be anonymous.

The Art. 6 of the Regulation determines that personal data processing is legitimate if certain conditions are met, and it states: "processing is necessary for the performance of a task carried out in the public interest". Therefore, when collecting data of public interest, it should be evident in the documents that it's precisely the public interest.

Unlike previous regulations, the GDPR explicitly states the issue of security of personal data processing, as explicitly stated in the Art. 32 of the Regulation: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 15,2025 at 01:37:26 UTC from IEEE Xplore. Restrictions apply.

organisational measures to ensure a level of security appropriate to the risk." Here, the GDPR enters into area which has so far been regulated by information security systems, by the series of standards ISO/IEC 27000. [8]

It should take into account that, especially in smaller places, even a regular video surveillance system may pose a threat to privacy according the GDPR. Let us recall the basic definitions of personal data, the Art. 4: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

By this definition, the natural person can be identified by the car which drives - if the place is small enough, and even in the city of tens of thousands of people, the car would be found by the colour and the vehicle type, even when driven by the single individual - then it can be recognized even without knowing the registration plates. In certain cases, if a surveillance footage comes into possession of a malicious person, a very serious privacy breach may arise.

VI. Conclusion

Does the application of the GDPR affect development of Smart City models? Already, *prima facie* on the basis of the analysis we can say that it affects. Today, the protection of personal data has been raised to a very high level in the EU, and since Smart City deals with people in their urban environment and by the quality of their life - personal data collection comes to as inevitable.

Should we be afraid of the GDPR? Not at all. Although, the beginning of the GDPR application has been related to the large marketing campaigns that offer various forms of education, the truth is, however, slightly different. The GDPR is upgrade of the existing regulation, and not a brand new document, or even a bureaucratically imposed document. An organization that has protected its personal data, by so far, and which has at least informal implementation of information security standards, will find that adapting to the new framework is just a step further, continuing of the existing regulation. An organization that showed ignorance to their personal data, or the personal data is the problem, certainly, within such organization a lot of effort will be necessary to adapt the Regulation.

Similarly, those who systematically started with the development of Smart City elements would not have any greater problems with the application of GDPR. Moreover, the GDPR can help to build a quality model of a Smart City. On the other hand, those who, by developing the Smart City model consider various partial forms of automation without a systematic approach, and development strategy – might be in trouble. It's enough to badly set a video surveillance of the traffic lights monitoring system, the personal data can then be abused in a small town.

What needs to be taken into consideration - various Big Data and similar models used in Smart City development are interested in processes and tendencies (e. g. road load per hour), rather than in natural persons and their personal data.

First of all, it's necessary, wherever is possible to use the pseudonymisation mentioned in Art. 4 of the GDPR: 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Certainly, the best policy is to use the full anonymity, in accordance with the Art. 89 of the GDPR: "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. (…) Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. Fully anonymous data cease to be personal data, as no natural person can be identified out of them.

There are also some aspects of Smart City projects which include personal data, such as participating in discussions in various models of micro-democracy, where the consent is given by the respondents themselves. In these cases, the high quality of application of ISO/EIC 27000 standards can come as a help.

In short, the GDPR shouldn't be seen as a ''danger''for the Smart Cities, but as a series of conditions which can be helful in the development of the Smart City models. Moreover, citizens will rather accept Smart City which will not remind them of some form of "Big Brother", or totalitarian control over their personal freedoms. Thus, the GDPR can also help in developing Smart City models, because its implementation guarantees a higher level of personal data protection, thereby reducing the fear of possible abuse of the control functions of the smart city.

References

[1] Official Journal of the European Union L 119/1, 4.5.2016

[2] Details of Treaty No.108: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (11 February 2018)

[3] Official Journal of the European Union L 281, 23/11/1995 P. 0031 – 0050

[4] *GDPR Key Changes* https://www.eugdpr.org/key-changes.html l (22 April 2018)

[5] Riva Sanseverino R., *Competitive Urban Models,* in Riva Sanseverino E., Riva Sanseverino R., Vaccaro V., Zizzo G. (ed.), *Smart Rules for Smart Cities*, Springer, Palermo, 2014, pp. 1-14

[6] Milenković, M., Rašić, M., Vojković, G., *Using Public Private Partnership models in smart cities – proposal for Croatia*, MIPRO 2017 Proceedings, Opatija, Croatia, pp. 1656-1661

[7] Surdean, R., *Secure Connections for a Smarter World*, MIPRO 2017 Proceedings, Opatija, Croatia, p. 5

[8] ISO/IEC 27000 family - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html (22. April 2018)

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 15,2025 at 01:37:26 UTC from IEEE Xplore. Restrictions apply.