DOI: 10.2507/31st.daaam.proceedings.xxx

JUDICIAL AND TECHNICAL IMPROVEMENT OF GENERAL DATA PROTECTION REGULATION

Vedran Dakic, Sanja Ribaric

This Publication has to be referred as: Dakić, V[edran]; Ribarić, S[anja] (2020). Judicial and technical improvement of General Data Protection Regulation, Proceedings of the 31st DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/31st.daaam.proceedings.xxx

Abstract

The issue of personal data protection of natural persons has been in the focus of the world public for years. Well-known data processors and controllers are often the target of attacks on their information systems, which is why personal data of millions of users ends up in unauthorized hands. After the adoption of the Regulation, an implementation vacuum arose due to vagueness, ambiguity and difficult readability of certain parts of the Regulation. In this paper, we will look at these uncertainties and ambiguities and propose practical solutions to improve the Regulation in legal and technical / security terms.
Keywords: privacy, security, GDPR, law, IT.

1. Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) took effect on May 25th, 2018 (hereinafter: Regulation). Just before the beginning of the application of this Regulation, we witnessed countless offers of education in the form of courses, seminars and lectures. At the same time, offered education offered almost nothing in terms of documentation, which is one of the key points of GDPR. We're yet to find a single education program that gives its students access to a real, complete package of template documents that need to be filled to get compliant. This was the first problem that we noticed - Regulation has a far reach in terms of "what it wants to be done", but almost nothing in terms of "how to do it" and "how to help companies do it".

The second problem is the fact that the Regulation introduces new, unclear and insufficiently defined terms for all those dealing with the processing of personal data on the one hand, and a threat of rigorous penalties for non-compliance with the Regulation on the other.

The Regulation requires, for example, controllers and processors to apply "reasonable measures", "appropriate technical and organizational measures", "adequate or appropriate safeguards", "reasonable fees", "ensure adequate security of personal data", without defining the terms in question, as well as when it comes to terms such as "without undue delay", "key interest of respondents", "legitimate interest", "disproportionate effort", "occasional processing", "extensive

processing", "regular and systematic monitoring of respondents to a large extent ","the likelihood that the breach of personal data will pose a risk to the rights and freedoms of the individual"[1]. It's full of terminology that's not explained properly, thus making it less understandable to regular people who need to implement it as this is not some kind of niche-based regulation - it applies to almost all of the EU companies.

This leads us to the third problem. In such circumstances, the assessment of compliance with the Regulation depends solely on the interpretation of the provisions of the Regulation and this practice that will take some time to harmonize, which is often unavailable to those liable to apply the Regulation. The application of regulations based on interpretation creates legal uncertainty as it gives supervisory authorities and courts too much freedom to assess the existence of a breach of the Regulation and to assess the amount of the penalty which can be considered "effective, proportionate and dissuasive" [1]., while everyone else doesn't get clear instructions for legitimate business operation.

The aim of this paper is to go through legal and information security issues with the Regulation, describe some of the unclear terminology from the real-life standpoint, and offer new ideas on how to change Regulation so that compliance with it becomes possible. We're basing our work - in large part - on our practical experience of actually working on GDPR compliance projects, over the span of the past three years. Also, we attended multiple seminars and education programs for GDPR, and that experience taught us a lot on the subject of problems that regular company owners will have with GDPR compliance.

2. Legal issues with the Regulation

Ignorantia iuris nocet (in translation - ignorance of the law is harmful) is one of the main principles of law and requires each of us to familiarize ourselves with legal regulations and act in accordance with them. The premise for this is that we understand what the regulations require of us. However, given the way legal regulations are written, this is sometimes difficult to understand for people with legal training, and very often almost impossible for those who do not have legal training. From the point of view of persons who do not have legal knowledge, additional difficulties in the application of regulations occur if they cannot find all the necessary information in one document or in one place, or if they are not familiar with the place and manner in which relevant information can be obtained.

This Regulation is an example of such a legal regulation with a multitude of professional, multidisciplinary, insufficiently clear and undefined terms that create legal gaps and require additional interpretation. In order to satisfy regulary requirements all organizations subject to GDPR need to conduct activites to adopt or modify their data usage, security and privacy policies [2].

That there is an awareness of the vagueness of the Regulation, the ambiguity of its provisions and the need for additional regulation to achieve legal certainty stems from the fact that the European Data Protection Board (EDPB) was established at EU level under Article 68 of the Regulation (hereinafter: the Committee). The Committee in question consists of representatives of national data protection authorities and the European Data Protection Supervisor, and its task is, among other things, to advise on personal data protection issues, issue guidelines, recommendations and best practices on issues regulated by the Regulation, review the practical application of these guidelines, recommendations and examples of best practice and, if necessary, their adaptation.

The Committee began its work on May 25, 2018, and by the end of 2019, it has published five guidelines that seek to provide clarifications and recommendations for controversial issues that have arisen in practice, which are related to:

- certification as a means of proving compliance with the Regulation [3],
- accreditation certification bodies [4],
- transfer of personal data to third countries [5],
- territorial application of the Regulation [6] and
- codes of conduct aimed at specifying how to apply the Regulation [7].

By the end of 2019, the Committee submitted for public discussion proposals for four further guidelines relating to:

- processing of personal data based on a contractual relationship with the respondent within the "online services" [8],
- processing of personal data via video devices [9],
- protection of personal data "by design" and "by default" [10] and
- the right to be forgotten in the search engine cases [11].

Until 25 May 2018, in accordance with Article 29 of Directive 95/46/ EC, which was repealed with the Regulation being enforced, the advisory role and tasks of providing guidelines, opinions and recommendations related to the protection of personal data of respondents were performed by the Working Group individuals in relation to the processing of personal data (Article 29 Working Party - A29WP; hereinafter: the Working Group).

At its first plenary meeting, the Committee endorsed sixteen documents previously drafted by the Working Group, including guidelines on:

- application and setting of administrative fines [12],
- determination of the leading supervisory body for controllers and processors [13],
- data protection officer [14],
- assessment of the impact on data protection and the likelihood that the processing will result in a high risk [15],
- the right of respondents to data transfer [16],
- notification of personal data breach [17],
- automated decision making and profiling [18],
- the principle of transparency [19] and
- consent [20].

Taking into account the scope and diversity of topics covered by the guidelines of the Committee and the Working Group, it is clear that the vast majority of terms in the Regulation are vague in themselves, which prevents its uniform application in practice and causes legal uncertainty.

For example, one of the terms not defined by the Regulation, and very important, is the term "high risk". The term is related to the obligation of the controller to keep records of processing activities, to conduct an impact assessment on personal data protection before processing, obliges to inform the respondent about personal data breach and to consult with the supervisory authority before processing. By non-performance or irregular performance of the stated obligations, the processing manager is exposed to misdemeanour liability and high fines.

The complexity of this concept is evident from the Guideline on Data Protection Impact Assessment and Determining whether Processing Procedures "Are Likely to Cause High Risk" within the meaning of Regulation 2016/679, adopted by the Working Group on 4 October 2017 and accepted by the Committee [15]. It follows from this guideline that when assessing the possibility of the occurrence of "high risk" it is necessary to take into account whether profiling is done, whether automated decision-making is used, whether there is systematic monitoring of respondents, whether it is sensitive data or data very personal in nature, whether it is extensive processing, whether it is matching or combined data sets originating from several types of processing, which have been carried out for several purposes and / or by several processing managers, whether it is sensitive categories of respondents, whether it is about the innovative use or use of new technologies and organizational solutions, and whether the processing itself prevents respondents from exercising their rights or from using the service.

The mentioned Guideline of the Working Group seeks to clarify the concept of "extensive processing" by proposing factors that need to be taken into account when assessing processing. The Working Party notes that when assessing the extent of processing, the number of respondents involved (either as a specific number or share of the relevant population), the amount of data and/or a range of different data processed, the duration or continuity of the processing and the geographical scope of processing activities should be taken into account.

The mentioned terms are new for the average controller and/or processor and it is difficult to expect that, by reading the Regulation, they will be able to independently determine which factors he must take into account when interpreting certain terms which expose them to the risk of misjudgement and unintentional Regulation violation.

By not defining, nor prescribing a framework from which it would be unequivocally clear what is considered reasonable, adequate, appropriate, disproportionate, etc., the Regulation puts taxpayers in a position to, even when acting in good faith and making every effort to be in compliance with requirements of the Regulation, they cannot be completely sure that their assessment and interpretation will correspond to the assessment and interpretation of the supervisory body that comes to them to supervise the business, i.e. the court in case of a dispute.

Insufficient precision of the Regulation is being compensated with aforementioned guidelines, recommendations, examples of good practice, binding decisions taken by the competent authorities, however, the same in practice only results in even greater legal uncertainty when considering the number of authorized bodies and the time necessary to harmonize their practices.

The Regulation has been fully applied since May 25th 2018., and new disputable issues arise on a day-to-day basis to which the Regulation itself does not provide a concrete answer, as a result of which a number of new interpretations and guidelines are expected in the future. However, until they are adopted, the path is open for legal uncertainty, both in relation to controllers and processors, and in relation to the respondents.

Also, although the aim of the guidelines is to facilitate the application of the Regulation, they often include concepts that are clear only to a small percentage of experts and require additional explanations.

Based on the analysis of the Regulation and its application in practice, we concluded that:

- for the average controller and processor, many terms from the Regulation are non-transparent and confusing, as well as the obligations imposed on them by the Regulation;
- that the average controller and processor does not know who is in charge of interpreting the Regulation and that opinions, guidelines, recommendations, best practices and binding decisions of public authorities are made public, available through their official website;
- some of the guidelines of the Committee and the Working Group have not been translated into other languages is another aggravating circumstance that puts some managers and processors in an unequal position.

In addition to the Committee and the Working Group for the Interpretation of the Regulation, national supervisory authorities, as well as the courts of the Member States of the European Union are therefore in charge of giving opinions, recommendations, guidelines and creating practice. An individual controller may be audited by a supervisory authority from any Member State of the European Union, and proceedings for breach of personal data of respondents may be brought before a court of any Member State of the European Union. The practice of the supervisory authorities and courts of the Member States, although being harmonized, does not have to be the same precisely because of the need to interpret the Regulation and may be completely inaccessible to the controller either physically or linguistically. Courts also publish their practice very rarely or not at all, which further complicates the consistent application of the Regulation.

Awareness of the complexity of personal data protection of respondents and the issue of interpretation and application of the Regulation stems from the fact that the Regulation prescribes that the Data Protection Officer must have professional qualifications, especially professional knowledge of law and practices in the field of personal data protection. No standardized form of professional development or certification so that persons who will become data controllers can become acquainted with the details of the implementation of the Regulation. There is no regulation of any periodic system of centralized informing of personal data protection officers or the public about news in the application, opinions, court judgments and the like. The consequences of such a lack of transparency are even greater when the structure and size of controllers and processors are taken into account. At the level of each EU member state, there are only a few percent of controllers and processors who have the human, time and financial resources to set up a team of people to implement the Regulation, which puts other processors and processors (usually SMEs) in very unequal market position, even when they have a desire to be in compliance with the Regulation.

Given the vagueness and ambiguity of the Regulation as well as the need to know the work and practice of all bodies dealing with the application of the Regulation, we consider it indisputable that the personal data protection officer must have legal knowledge. However, in today's digital age, when a large part of the personal data of respondents is processed through computer systems, for the application of the Regulation we consider the principles and scope of information technology knowledge equally as important, as well as application of both in practice. With this in mind, we believe that it is necessary to formally educate data protection officers as well as to organize a system of regular testing of their knowledge, in order to keep abreast of evolving and changing practices.

3. Regulation information security issues at the technological implementation level

The issue of the Regulation continues in the technological implementation of the Regulation in terms of information security of information technology systems, as the Regulation prescribes unclear rules on the application of various security technologies. At the same time, the Regulation in some way imposes an obligation to introduce an information security management system similar to that introduced by ISO 27001 or 27002 standards. However, there are significant differences between the Regulation and ISO 27001/2 standards. Based on the conducted analysis, we have identified several areas in which the stated standards and the prescribed requirements of the Regulation differ:

- ISO 27001/2 and similar standards are optional standards that managers and processors introduce to bring their business into line with some internationally accepted standards for information security (i.e. for internal reasons), or to prepare for a more competitive market presence (for business reasons), where business reasons often prevail, when such standards are introduced, i.e. in order to comply with the conditions of various business tenders, which is why there is no legal obligation to introduce ISO 27001/2,
- ISO 27001/2 standards have very detailed measures and criteria introduced by specialized, educated and authorized persons who have taken complex exams before certification bodies in order to become auditors (auditors) of information security, while this is omitted by the Regulation as a result of which most controllers and processors blindly "bought" low-quality documentation from the Internet in order to "comply" with the Regulation as soon as possible,
- ISO 27001/2 standards require significant material investment in terms of recording business processes of controllers and processors, technological solutions, preparation of documentation and employee time, but this is in itself in the DNA of such standards. The regulation imposes such a way of thinking on all controllers and processors.

- Due to the obligation to comply with the Regulation, which by the start date of application did not bring almost any assistance to taxpayers (documentation, interpretations, active prescribing of necessary standards, minimum technical and safety standards for compliance), a number of harmful phenomena occurred in terms of quality compliance with the Regulation;
- Due to the complexity of the topic and the associated costs, most controllers and processors decided to do all the steps independently, and as audits, risk analysis and similar procedures require extensive knowledge of processes and procedures (often undocumented) and even more extensive legal knowledge, in fact the majority of controllers and processors have been put in the position that from the very start, the compliance with the Regulation they will be based on the wrong premises, and thus come to wrong or semi-accurate conclusions,
- Due to previously mentioned facts, a large number of persons or legal entities offering services for establishing compliance with the Regulation appeared on the market, and there were cases when experts "proved" their knowledge with non-existent and unofficial certificates, both via projects for establishing compliance with the Regulation, as well as via trainings where certificates for personal data protection officers were awarded.

Such situations could have been easily avoided, through the publication of minimum concrete standards, the documentation that controllers and processors have to go through and the certification of personal data processing officers in order to be able to comply with the provisions of the Regulation with certainty. This would prevent further deterioration in the compliance quality and address a lot of grey areas for decisions that follow from the potentially subjective understanding of parts of the Regulation by legal entities on the one hand and regulatory agencies on the other.

Let's illustrate the analysed topic on a simple example. We're deliberately trying to use one of the most widely used examples to illustrate the problem. A company (controller and processor) uses shared Internet access for employees' computers, a web store where it sells its products for which it offers to send promotional materials via marketing e-mail list, a wireless computer network used by employees to connect to business network and the Internet and an external accounting service to which documents are sent partly physically (paper) and partly through e-mail. Also, employees are provided with remote access to the infrastructure through PPTP (*Point-to-Point Tunnelling Protocol*) or SSTP (*Secure Socket Tunnelling Protocol*) VPN (*Virtual Private Network*) connection. This is one of the examples where the Regulation completely fails to use its power as an element of raising the quality of information security at its most basic level.

The application of "appropriate organizational and technical measures" is required, without knowing what this specifically means. We see no reason why the Regulation does not prescribe what the minimum level of security is - what kind of wireless encryption technology (i.e. insist on a minimum WPA2-Enterprise that uses certificates and ban WEP and WPA protocols that are insecure as it's been well documented)[20][21], why there was no insistence on at least minimal network security measures (install a firewall on the network, all computers or both) and why isn't it mandatory that some file encryption technology must be used to send files with personal data of private persons via e-mail. In terms of VPN connection, it could be prescribed to prohibit the use of insecure PAP and MS-CHAP authentication systems (*Password Authentication Protocol*, *Microsoft Challenge Handshake Authentication Protocol*) [23], as well as some types of insecure VPN connections (i.e. PPTP or SSTP) [22]. There are also known attacks on IPsec (*Internet Protocol Security*) IKE (*Internet Key Exchange*) and SSTP VPN connections [24][25]. All the mentioned authentication systems and VPN connections have a number of security vulnerabilities that can easily lead to data leaks, including personal data.

The example given is actually an example that can be scaled to a controller or processor of almost any size, as Internet presence and especially remote connectivity is something that became even more important with the COVID-19 pandemic situation.

We are very aware of the fact that us saying that the Regulation needs to "prescribe" security minimums will potentially lead to objections of excessive administrative meddling. The simple fact is - we should keep in mind that it is almost impossible to buy a wireless access point without WPA2-Enterprise mode (with authentication through a certificate) and a computer without operating system firewall. In terms of sending files via the Internet, it can be done securely by setting passwords on the files themselves or file archives. From the aspect of VPN connections, it could be recommended to use the L2TP protocol (Layer 2 Tunnelling Protocol) with authentication via certificates, since all protocols that use PSK are vulnerable (Pre-Shared Key). All of these technologies are available for no additional costs.

The obligation to use business user certificates to sign documents containing personal data and sent via the Internet could also be introduced as it's nothing new. Using our example as a basis, further research needs to be made to analyse if there's a way to minimize the use of personal data in accounting business processes, and if not, what can be done to protect personal data from leaking [26]. A typical example of why personal data is sent via the Internet in everyday business are e.g. business trips (sending data on an employee going on a trip to a travel agency), communication with external accounting services (sending invoices in PDF format for expense claims, salary processing, etc.). Services that use digital certificates for signing documents in the EU already exist in practice, i.e. in the communication of lawyers with the courts in proceedings before the Commercial Courts. Thus, the vast majority of the proposed measures actually boil down to reconfiguring pre-existing technologies, without any additional financial investment. It would require some time to set up

security systems appropriately. But it would already be a big qualitative shift in the direction of improving the level of communication security in such everyday situations.

A particularly sensitive area of the described example is the use of web stores and marketing lists to sell services and communicate with customers. Compliance with the Regulation becomes very complicated and depends on a number of parameters - whether the legal entity and the private person already have a previous business relationship, whether there is a legal obligation to ask for personal data, whether the legal entity uses technologies to monitor customer tracking while using a web store, whether tracking data is used for some form of automated processing, or profiling etc. Due to the complexity these concepts, controllers and processors either took the risk and left everything as it was before the Regulation - since everything else is too demanding and too expensive - or applied consents as the "only" way to insure against non-compliance. In practice, there's an abundance of cases of conditional use of services with mandatory consent or forcing a non-existent legitimate interest with a failed or incorrectly conducted proportionality test. What data controllers and processors need is a clear guidance on when to implement these mechanisms, explained in simple terms. Then it makes sense to leave it in the hands of auditors from governing bodies to check whether or not these guidances have been implemented correctly.

One of the frequent and definitely the most complex examples of the implementation of the Regulation in practice is the use of personal data of users from various databases for testing in application development processes. Prescribing that a publicly available test database with randomly generated data at the level of the entire European Union must be used would significantly reduce the possibility of personal data leaks from test environments, as test environments are often less protected from security attacks than real, production environments. Using known and publicly available test databases created by Microsoft and the authors of this paper, we created one of the test databases with randomly generated user data in XLS and .bak format for Microsoft SQL Server. Such content could be easily upgraded by the controller or processor for internal purposes, if an extension with additional data types is required. At the overall Regulation implementation level, one could approach the development of a simple online application that would allow easy creation and addition of additional content, recording content in CSV format, which is easily converted to XLS format and loaded into databases. We mention this only as an example of a simple procedure that only takes minutes, that can greatly help processors or processors who develop applications to comply with the provisions of the Regulation.

4. Further elaboration on the subject of introducing mandatory education and certification for data protection officers

There are many different areas in which a country, using its ability to implements laws and regulations, uses that power for the greater good. Some examples include ensuring quality of people/experts working in areas of architecture, building industry, education, health services etc. All of these activities require passing of additional exams to ensure candidate's familiarity with law, norms, technologies, procedures etc. It's a simple fact that a person can't be a heart surgeon unless he or she attends medical school, does residency, passes additional exams and then - and only then - can that person perform a heart surgery. Similar procedures apply to other aforementioned activities, albeit a bit simpler procedure.

In the 21st century, the greatest wealth - or the most important priority of any business - is to have access to relevant information. It's only normal that business will do a lot to get access to information, which includes personal information about end users, customers etc. This is why companies like Facebook, LinkedIn, Google, Apple, Microsoft and others put such a big priority on getting access to the data, so that they can use the data to their own benefit. It's in the nature of business to do so and as long as they're doing that in accordance with the law, there should be no problems.

The problem that keeps happening in the past five to ten years is the fact that these and other companies, and even governments are selling, reselling, buying, manipulating and mis-using that data, and trying to use it with only their benefit in mind. This is why data privacy laws were introduced all over the world, including the EU. Some legal frameworks that were created so that data can be shared in accordance to the law have been struck down by the courts. The biggest example of that was the EU-US Privacy Shield, which was struck down by the European Court of Justice in July 16th, 2020. This only goes to shows us that we need work from the ground-up (regular people all the way to people creating laws), not only from the top-down (the other way around). And the only way to introduce a ground-up change to situations like these is by educating people so that they know what's right, and what's wrong.

It's therefore completely baffling that the Regulation didn't create some sort of educational and certification framework for key people in the information security scheme mandated by the Regulation - Data Protection Officers. As explained earlier, there are so many other examples where laws did that for a variety of other activities. On top of that, there are so many educational programs verified by EU governments that claim to teach people about information security. There are different levels of ISO 27001 training (Implementer, Auditor, Internal Auditor, Foundations etc.). There are other ISO 27000 certifications (27002, 27004, 27005) that go even deeper into the subject - implementation, measurement of information security, security risk management, etc. It makes no sense that these certifications are available for practically

the same topics if a person wants to be an ISO auditor, while no official, mandated certifications were created for GDPR compliance. There are other programs - for example ISACA's CISA, Certified Information Systems Auditor. Just as an example, a person that passed CISA, with external or internal help of a lawyer would make a very strong team to implement GDPR. Other programs (PECB, EUGDPR) could also be further evaluated, modified and changed to form a core of official GDPR certification. We're using PECB and EUGDPR just as examples of programs that claim to be DPO certifications, while obscuring the fact that there is no DPO certification. We mentioned this problem previously in this paper.

5. Conclusion

On the one hand, the regulation requires multidisciplinary knowledge, strict formalism, in-depth analysis of business processes of processing managers, detailed and up-to-date keeping of numerous records, continuous education and testing of employees' knowledge and actions, supervision of data processors, introduction of appropriate security measures etc. Requests towards controllers and processors are numerous and extensive, while at the same time the compliance assessment is left in the air, due to insufficient definition of key concepts and obligations. This opens the way to arbitrariness and legal uncertainty.

It is undeniable that it is impossible to prescribe solutions in advance for every situation that may occur in practice, but given that every data controller and processor is obliged to act in accordance with the Regulation, we believe that the Regulation needs to be heavily updated so that compliance becomes an achievable, realistic goal. We consider it necessary to define the terms covered by the Regulation in such a way as to be comprehensible to persons who have no prior knowledge in the field of law and information technology, and, on the other hand, to provide clear, specific and verifiable criteria for assessing compliance.

In this way, doubts in the actions of the controller and processor will be removed, and respondents will be provided with adequate protection of their rights.

For this reason, we believe that in order to improve the Regulation and its implementation, it is necessary to take the following steps:

- do a comprehensive update of the Regulation so that the average person can understand it, which means that it is necessary to clarify all terms that are not well defined by the Regulation,
- prescribe the mandatory certification of persons who will perform the duties of personal data protection officers,
- form a centralized information system on novelties in the implementation of the Regulation - based on opinions, guidelines, recommendations, examples of best practice, court rulings, etc.,
- focus on feasibility for all controllers and processors, not just those who may have a team of people for the compliance process (large companies),
- create a centralized online service for creating test data so that testing in application development is conducted on test, and not on real personal data of respondents,
- prescribe minimum technical and security measures, in clear language,
- prescribe the minimum required security standards for the most commonly used services such as wireless access, remote access via virtual private networks, etc.,
- translate the documents of the Committee and the Working Group to all EU member languages at a greater speed so that controllers and processors, as well as respondents from all of the EU countries, can have equal access to all relevant decisions of these bodies.

We firmly believe that implementing these steps would go a long way towards making GDPR compliance a possibility, not an unachievable myth. Further research can be done in terms of comparing various regulatory body practices across the European Union, as these practices should be standardized. Also, research can be done on the topic of how to implement GDPR compliance for a variety of different business entities, especially with fast-changing environments (due to regular change cycle and COVID-19 pandemic) - like education sector, work from home, wide-spread usage of various biometric technologies (video-surveillance, thumbprint scan). Manufacturers of modern smartphone devices commonly use fingerprint recognition to access more expensive devices [26], for example, to create one-time passwords for VPN connections, e-banking solutions etc. The question is – does that data leave the device, where, why, and what is it being used for?

Furthermore, new research needs to be done because of the fact that Privacy Shield can't be used as a framework to cover data export to USA as this fact will significantly change the way companies work with data.

5. References

[1] EPDB (2016). 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), Bruxelles.

[2] EPDB (2018). Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Bruxelles.

[3] EPDB (2018). Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Bruxelles.

[4] EPDB (2018). Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), Bruxelles.

[5] EPDB (2019). Draft administrative arrangement for the transfer of personal data between each of the European Economic Area, Bruxelles.

[6] EPDB (2019). Guidelines 3/2018 on the territorial scope of the GDPR, Bruxelles.

[7] EPDB (2019). Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Bruxelles.

[8] EPDB (2019). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Bruxelles.

[9] EPDB (2019). Guidelines 3/2019 on processing of personal data through video devices, Bruxelles.

[10] EPDB (2020). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Bruxelles.

[11] EPDB (2020). Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1), Bruxelles.

[12] A29WP (2017). Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Bruxelles.

[13] A29WP (2017). Guidelines for identifying a controller or processor's lead supervisory authority, A29WP, Bruxelles.

[14] A29WP (2017). Guidelines on Data Protection Officers ('DPOs'), Bruxelles.

[15] A29WP (2017). Guidelines on Data Protection Impact Assesment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679, Bruxelles.

[16] A29WP (2017). Guidelines on the right to data portability, Bruxelles.

[17] A29WP (2017). Guidelines on Personal data breach notification under Regulation 2016/679, Bruxelles.

[18] A29WP (2017). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Bruxelles.

[19] A29WP (2017). Guidelines on transparency under Regulation 2016/679, Bruxelles.

[20] A29WP (2017). Guidelines on consent under Regulation 2016/679, Bruxelles.

[21] Tews, E., Weinmann R., & Pyshkin, A. (2007) „Breaking 104-bit WEP in less than 60 seconds“, Lecture Notes in Computer Science vol. 4867., Korea.

[22] Beck, M. Tews, E. (2009) „Practical attacks against WEP and WPA“, Proceedings of the second ACM conference on wireless security, Zurich.

[23] Scheiner, B., Mudge, (1998) „Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)“, Proceedings of the 5th ACM conference on Computer and communications security.

[24] Felsch, D., Grothe, M., Schwenk, J., Czubak, A. & Szymanek, M.(2018) „The Dangers of Key Reuse: Practical Attacks on IPsec IKE“, Proceedings of the 27th USENIX Security Symposium, Baltimore.

[25] https://nvd.nist.gov/vuln/detail/CVE-2020-0601, (2020). CVE-2020-0601, Accessed on: 2020-08-30

[26] Vojković, G., Milenković, M. (2018) „GDPR in access control systems and attendance systems using biometric data“, MIPRO, ISBN 978-953-233-095-3, Opatija.

[27] Marinclin, A., Mikic, I. (2018) „Application of GDPR in higher education: Example on library and accounting”, 6th Inernational Conference “Vallis Aurea”, Daaam International Vienna and Veleučilište u Požegi, ISSN: 1847-8204, Požega