TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Marleena Jokinen

THE IMPACT OF THE EUROPEAN UNION DATA PROTECTION REGULATION 2016/679 ON THE FINNISH PERSONAL DATA ACT

Bachelor's thesis
Programme HAJB08/14 International Law, specialisation European Union Law

Supervisor: Jenna Uusitalo, MA in Law;
Ph.D Candidate at Uni. Helsinki

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 7641 words from the introduction to the end of summary.

Marleena Jokinen

……
(signature, date)

Student code: 156149HAJB
Student e-mail address: marleena.jokinen@gmail.com

Supervisor: Jenna Uusitalo, MA in Law; Ph.D Candidate at Uni. Helsinki:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defense Committee:
Permitted to the defense

……
(name, signature, date)

ABSTRACT

The research examines current Finnish legislation regarding the Personal Data Act and compares it with the requirements of the Data Protection Regulation 2016/679. The purpose is to find out how the European Union's Data Protection regulation will impact to the current Finnish Personal Data Act and how the law will be amended. The hypothesis is that the Finnish Personal Data Act needs to be clarified in accordance with the Regulation. The research method is legal research. The information will be collected from different science books, articles, and legal acts. The research will be qualitative. According to the research, the hypothesis was right; The Finnish Data Protection Act needs to be clarified in accordance with European Union's General Data Protection Regulation.

Keywords

European Union, General Data Protection Regulation, Finnish Personal Data Act

TABLE OF CONTENTS

1. **INTRODUCTION**

On 24th of October 1995 European Union draft the Data Protection Directive 95/46/EC. The Directive was regulating the processing and movement of personal data, and the aim was to harmonize the data protection laws and transfer the personal data to the third countries.[1] However, in 1995, technology was not as advanced as it is today; for example, social media was familiar only for a fraction of the European population. The technological development posed problems with the protection and processing of personal data, and in 2012 the European Commission proposed a new updated law.

In Spring 2016, after four years debate and preparation, the Council of the European Union and the European Parliament adopted the General Data Protection (GDPR) regulation, which would replace the 1995 Personal Data Directive.[2] The purpose of the General Data Protection Regulation is to update data protection legislation in order to meet the challenges of technological development and the protection of personal data related to globalization. It is also intended to support the development of the digital economy in the internal market by harmonizing Member States' data protection provisions and building trust[3]. The General Data Protection Regulation will be enforced in May 2018[4].

This research focuses on the impact of the new Data Protection Regulation and possible changes to the Personal Data Act from the point of view of the Finnish legislation. The aim of the research is to find out how the European Union's Data Protection Regulation impact to the Finnish Personal Data Act. The research question is:

[1] Directive 95/46/EC
[2] Talus, A., Autio, E., Hänninen, A., Pihamaa, H. T., Kantonen, S. (2017). *Miten valmistautua EU:n tietosuoja-asetukseen*? Helsinki: Oikeusministeriö. (How to prepare for the GDPR?)
[3] Finnish Ministry of Justice (2017): *Implementation of the EU Data Protection Directive OM005: 00/2017 LEGAL PREPARATION*
[4] Albrecht, J. P. (2016). How The GDPR Will Change The World. *European Data Protection Law Review.* p.287

1. How will the General Data Protection Regulation 2016/679 impact to the Finnish Personal Data Act?

In addition, the sub-study question has been used to facilitate the description of the problem:

2. How much the Finnish Personal Data Act need to be changed?

Technology has developed significantly since 1995. Therefore, my hypothesis in my research is that the Finnish Personal Data Act need to be clarified in accordance with European Union's General Data Protection Regulation 2016/679.

The thesis is proceeding so that the second chapter deals with European Union's General Data Protection Regulation, its concept and the requirements of the Regulation. The third chapter deals with the Finnish Personal Data Act; what is the current state, what parts it consists of. The fourth chapter process the requirements of the Regulation 2016/679 comparing to the Finnish Personal Data Act, sections, that need change and how the sections need to be changed. The fifth chapter draws a conclusion. Finally, the summary will summarize the research.

2. EUROPEAN UNION DATA PROTECTION REGULATION 2016/679

The European Union's development began in the 1950 century when the European Coal and Steel Community (ECSC) was set up. The aim of the ECSC was to develop economic and political cooperation and to end the recurring wars in Europe.[5] In 1957, the Treaty of Rome was signed, establishing the European Economic Community (EEC), i.e. the common market. Development continued, in 1993 the creation of a single market was completed and the goods, services, people, and capital were allowed to move freely in the area. [6]

[5] Vataman, D. (2010). Lex ET Scientia International Journal. *History of the European Union,* Vol. 17, Issue 2), 107-109

[6] Craig, P. de Burca, G. (2015). *EU Law: text, cases, and materials, sixth edition*

At an early stage, the Court of Justice of the European Union (CJEU) stated, that the European Union's legislation goes beyond the national law, on the other words States have to comply with EU directives and regulations. According to the Article 289 (1) TFEU, a legislative act can be adopted in the ordinary legal procedure, which consists in the joint adoption by the European Parliament, and the Council of a regulation, directive and decision on a proposal by the Commission in conformity with the Article 294 TFEU.[7] Regulations are acts, which apply automatically and equally in all Member States immediately upon their entry into force. The regulations bind all Member States in their entirety[8]. Directives oblige the Member States to achieve the objectives set out in the directives, but the countries themselves decide on the means to be used. Member States have to transpose the Directives into national law.[9]

2.1 Data Protection as a Human Right

In Europe, Human Rights were born after the Second World War and it entered into force in 1953[10]. The rights are international rules, that are defined by international agreements and declarations[11]. The basis of current human rights thinking is closely linked to the political development in the Europe[12]. Human rights are parts of international laws and are enshrined in international human rights conventions. International agreements define the minimum level that States have to comply with their national legislation.[13] The European Convention on Human Rights is one of the most important agreements in Europe, and it is nowadays considered to be legally binding it the EU, even if the EU is not really a Human Rights organization[14].

Article 8 of the European Convention on Human Rights regulates the Right to respect for private and family life[15]. Even if the protection of private and family life is defined briefly in the

[7] Biondi, A., Eeckhout, P., Ripley, S. (2012). *EU after Lisbon*. p. 67
[8] Steiner, J., Twigg-Flesner, C., Woods, L. (2006). *EU Law, 9th edition.* United Kingdom: Oxford University Press.
[9] Robinson, W. (2010). Manuals for Drafting European Union Legislation. *Legisprudence*, Vol 4, Issue 2, 129-156.
[10] 13. Finch, V., McGroarty, J. (2010). *Human Rights.* Dundee: Edinburgh University Press.
[11] Van der Vyver. (1979). The Concept of Human Rights: Its History, Contents and Meaning. *Acta Juridica*, Vol 1979, 10-32.
[12] Frost, W L. (2000). The Developing Human Rights Discourse: A History of the Human Rights Movement. *Trinity Law Review*, Vol 10, 1-3
[13] Letsas, G. (2007). *A theory of interpretation of the European Convention on Human Rights.* Oxford: Oxford University Press.
[14] Douglas-Scott, S. (2011). The European Union and Human Rights after the Treaty of Lisbon. *Human Rights Law Review*, Vol 11, Issue 4, 645-682.
[15] Reijneveld, M. (2017). A Journal of Law, Technology and Society. *Quantified Self, Freedom and the GDPR.* P.288

agreement, it is applied very often and broadly. The right to protect the person and his home and family; information about any private matter can not arbitrarily be deployed either. [16] Nowadays, Human Rights protection and promotion are very important part of the European Union's identity. Respect for human rights is also one of the fundamental values binding on the Member States of the European Union[17]. According to the Article 7 of the EU Treaty, violation of the rights might lead to a temporary suspension of the membership rights.

2.2. The Concept of the EU's Data Protection Regulation

Currently, the right to data protection in the EU is regulated in the Directive 95/46/EC. The Directive protects individuals with regard to the processing of personal data and also the free movement of such data.[18] The principles and objectives of the Directive remain sound, but it seems that there is still considerable fragmentation in the EU, in particular, legal uncertainty. Different views of the Member States on the protection of personal data may constitute an obstacle to the Union's economic activity, distort competition and prevent the authorities from carrying out their obligations under Union law.

The European Union has always seen to be very coherent and trusting economic and political alliance, therefore the legislation should also be up-to-date. The globalization of the world and very rapid technological development are the main reasons, why the current data protection directive is questioned nowadays. The importance of personal information has increased; more and more are shared and collected personal data for various purposes, and technology makes it easy and very extensive to use personal data[19]. Therefore, in Spring 2016, the Council of the European Union and the European Parliament adopted the General Data Protection Regulation (GDPR).

[16] Lambert, S., Lindsay-Strugo, A. (2008) Focus on Article 8 ECHR:Recent Developments. *Judicial Review*, Vol. 13, Issue 1, 29-40

[17] Craig, P. de Burca, G. (2011). *The evolution of EU Law*. Oxford ; New York : Oxford University Press. P. 495

[18] Allisom, S. (2009). The concept of Personal Data under the Data Protection Regime. Edinburgh Student Law Review, Vol 1, Issue 1, 48-65

[19] Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, Vol. 47, Issue 3, 809-810

The General Data Protection Regulation (GDPR) will replace the current Data Protection Directive 95/46/EC and will be applicable in all Member States. The aim of the regulation is to update the data protection legislation in order to meet the challenges of technological development and the protection of personal data related to globalization. One major reason for the delays in cross-border exchanges of personal data between public and private actors in the Union, such as natural persons, organizations and businesses, is the economic and social integration of the internal market.[20] Hereford, it is also intended to support the development of the digital economy in the internal market by harmonizing Member States' data protection provisions and so increase trust between the States. [21]

The purpose of the GDPR is also to increase the transparency of the processing of personal data and to strengthen the rights of data subjects to control the processing of their personal data. The Regulation provides for stricter penalties for the processing of personal data contrary to the Personal Data Act. Therefore, people will have more rights to their personal information, including now also information about different online identities, location information, and biometric data. A customer can, for example, ask that the organization needs to provide a report, which includes a description of all personal information that the organization has in their records. Customer may also require a company or organization to remove or relocate any personal information about him. The company must also be able to prove that the data has actually left or moved.

According to the earlier chapter, the Data Protection Regulation applies to all personal data processing organizations that are covered by it, both data controllers and personal data processors. The scope of the Regulation is limited by its provisions concerning the substantive and territorial scope. It will also apply to organizations established outside the EU in certain situations, which are defined in the Regulation. The Regulation applies in both the private and public sectors, regardless of the extent of the processing of personal data, the nature of the personal data being processed or the technology used.[22]

[20] Ferretti, F. (2016). The Foundations of EU Data Protection Law. *European Data Protection Law Review (EDPL)*, Vol. 2, Issue 2, 278-280.
[21] Talus, A., Autio, E., Hänninen, A., Pihamaa, H. T., Kantonen, S. (2017). *Miten valmistautua EU:n tietosuoja-asetukseen*? Helsinki: Oikeusministeriö. (How to prepare for the GDPR?)
[22] Voigt, P., Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*.

Mostly the General Data Protection Regulation has five goals; more rights for citizens, new obligations for the controller, wider powers to the authorities, strong, unified and comprehensive data protection for the European Union and to develop an internal digital market.

2.2. Requirements of the Regulation

2.2.1 The processing of the personal data

In principle, according to the section two of the Regulation, the processing of the personal data should always protect the data subject's right to protection of personal data and their fundamental rights and freedoms, without questioning their nationality or the residence. Processing of personal data should be legitimate and appropriate. Also, according to the Article 28 (1), where processing is to take place on behalf of the controller, the controller shall only use personal data processors, who take adequate safeguards to implement appropriate technical and organizational measures so that the processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject.

Based on the Article 12 (1) of the Regulation, the information and communication related to the processing of personal data must be easily accessible and understandable and the language must be clear and simple, on the other words the processing of the personal data should be transparent. The specific purposes of handling personal data should always be determined and reported to the data subject.

According to Article 5 of the GDPR, the personal data should only be processed for the purpose intended. Therefore the retention of the personal data will be as short as possible. Personal data should be processed in such a way as to ensure the proper security and confidentiality of personal data. That will provide unauthorized access to personal data or equipment used for processing them, and unauthorized use of such information or equipment.

In principle for the processing of the personal data, there should always be a permission of the data subject. However, based on Article 6 of the Regulation, the processing is legitimate without data subject's permission, when it is necessary to protect the interests of a registered or another natural person, for example in the event of a traffic accident, where the patient is a danger of

death (medical information). However, according to Article 8, if the data subject is a child, processing of the child's personal data is legal if the child is at least 16 years of age. If the child is under 16 years of age, such treatment is only lawful in the case and insofar as the consent of the child's parent or guardian has been granted. Member States may provide for a lower age for this purpose, which may not be less than 13 years in their legislation. The processing of sensitive data (Article 9); personal information, which is particularly sensitive to fundamental rights and freedoms, should be processed particularly carefully.

2.2.2 The rights of the data subject

The Data subject is defined as a physical person, implying that others, for example, public authorities are not data subjects and therefore not covered by data protection law[23]. The section three of the GDPR regulates the rights of the data subject. One of the controller's responsibilities is to enforce the rights of the data subject. The Data Protection Regulation emphasizes the transparency of the processing of personal data and provides more detailed rules on the implementation of the data controller's duty to inform the data subject, why personal data is processed and what are the rights of the data subject. The controller shall provide to the data subject the aim of processing of the personal data in easily understandable and accessible form. According to the Article 13, information on the measures taken following a request from a data subject should be issued without undue delay and no later than one month after the receipt of the request. The Regulation provides information on how to register the data in situations where personal data is collected directly from the data subject and, on the other hand, in cases where the personal data is collected from a non-registered user (Article 13).

Based on the Article 14, the Regulation defines a more precise deadline for the disclosure of personal data when the collected personal data is not registered. Information on the processing of personal data must be submitted within a reasonable time, but no later than one month after the receipt of personal data. If the information is used for communication with the data subject, the information must be provided at the latest when this information is first disclosed.

[23] Blume, P. (2015). The Data Subject. *European Data Protection Law Review*. p.258

According to the Articles 16 and 17 of the Regulation, the Data Protection Regulation gives the data subject with certain exceptions the right to rectify the data and to remove the right to information, ie the so-called right to be forgotten. Similar rights are also included in the Personal Data Act, although the right to be forgotten is not explicitly included in the Act. The Regulation lays down also the controller's obligation to notify data controllers handling personal data that the data subject has requested the deletion of personal data links or copies of such personal data.[24] The Personal Data Act also includes the obligation to notify the person to whom the data controller has disclosed or from whom the data controller has received personal data.

Based on Article 18, the Data Protection Regulation also provides for the right to limit the processing. The registrar has the right to have active treatment restricted in the four different situations listed in the Regulation. There is, for example, a right where the data subject submits a request for rectification or removal of personal data and therefore disputes the accuracy of personal data. Methods for limiting the processing of personal data may include, for example, transferring selected data to another processing system or accessing user access to selected personal data.

According to the Article 20, the data subject has the right to transfer personal data concerning him to the data controller from the registrar to another, without prejudice to the data controller to whom the information was provided. The data must be transferable in structured, commonly used and machine-readable form. The data subject has the right to have personal data transferred directly from the controller to the other if it is technically feasible. However, an authorized person is entitled to a transfer only if the processing is based on consent or agreement and if the processing is performed automatically. The data subject's right to transfer data from one system to another shall not be subject to the processing required to perform a public interest task or to exercise public authority under the control of a controller. Neither the right of the registered user nor the rights and freedoms of others shall be adversely affected.

[24] Gutwirth, S., Leenes, R., Hert, P. (2015). *Reforming European data protection law.* Dordrecht: Springer. P. 203-205

2.2.3 Transfer of personal data

Cross-border transfers of personal data to third countries, to international organizations and back to the Union have increased, because of the international trade and cooperation. Because the transfers of personal data have increased considerably it also concerns about the protection of personal data have increased. None of these transfers should endanger the level of protection of personal data of natural persons. [25] Transfers to third countries and to international organizations may, in any event, only be made in full compliance with this Regulation. However, this Regulation shall not affect international agreements concluded between the Union and third countries, provided that the controller and the processor comply with this Regulation.

According to Article 44 of the Regulation, the transfer of personal data to third countries to international organizations, and to the Union may be legal only if the controller and the processor are acting in accordance with the fifth chapter of the Regulation.

Personal data may be transferred to the country concerned without further permission if the Commission has made a decision, that a certain third country or a particular region or sector in a third country or a particular international organization provides a sufficient level of data protection and thus ensures legal certainty and consistency. The Commission is also able to repeal its decision, if the Commission notifies the matter and gives reasons to another part.

If the Commission has not made a decision about the transfer of personal data, the transfer is legal only if the controller or the processor of the personal data has taken the appropriate safeguards and if there are enforceable rights and effective remedies available to the data subject.

2.2.4 The position and tasks of the Data Protection Officer

The section four of the GDPR, regulates the aim of the Data Protection Officer. According to the Article 37 (1, a), the controller and the personal data processor shall appoint a Data Protection Officer, when processing is carried out by another Authority or by a body governed by public

[25] Goldberger, D., Akerman, N., Levin, J., Ray, D. (2017). Cross-Border Data Privacy Issues. *Cardozo Journal of International and Comparative Law*, Vol 25, Issue 2, 379-vii.

law (other than the court in its jurisdiction). The Data Protection Officer should timely and adequately be part of the processing of all personal data protection issues.

The Data Protection Officer provides information and advises to the controller or to the processor of the personal data processing concerning their obligations. The officer will also monitor compliance with this Regulation and cooperate with the supervisory authority, based on Article 39 of the Regulation.

2.2.5 The consequences of abuse

The controller and the personal data processor, as well as, where appropriate, the controller or personal data handler representative shall, on request, cooperate with the supervisory authority to carry out his tasks, based on the Article 31 of the Regulation.

The security breach may result in physical, material or intangible damage to natural persons such as loss of control of personal data or limitation of rights. According to Article 33 of the Regulation the controller should inform the supervisory authority of the breach of personal data without undue delay as soon as he has become aware of the controller and if it is possible, within 72 hours, provided, that the controller can not indicate, that personal data security breach is unlikely to give rise to a risk to the rights and freedoms of natural persons. The controller should inform the data subject as soon as possible.

In case of violation of provisions of the Regulation, the penalty might be fine, or note if the breach is minor. The penalty can also be other measure imposed by the supervisory authority. The severity of the punishment depends among other things the nature, severity and duration of the infringement and its intent, in any case, Authorities should judge the punishment taking also those factors into account.

The Member States has right to determine the rules of punishments. However, the punishments should be in accordance with the general principles of the Union law and the Charter of Fundamental Rights.

3. FINNISH PERSONAL DATA ACT

3.1 Current state

The Personal Data Act (523/1999) provides for the protection of privacy and other fundamental rights protecting personal privacy when processing personal data and to promote the development and observance of good data processing practices.[26]

The law applies to the automatic processing of personal data as well as to other personal data processing when personal data is intended to constitute a personal register or part thereof. However, the Act does not apply to the processing of personal data by a natural person solely for personal or comparable normal private purposes, nor for the processing of personal data for editorial purposes and for purposes of artistic and literary expression.

The Personal Data Act regulates the general conditions for the processing of personal data, the obligations, that must always be met in the processing of personal data, the rights related to the processing of personal data, the application of the law enforcement system, and sanctions that may follow the processing of personal data. The law regulates, among other things, in which cases personal data can be processed without the consent of the data subject.[27]

3.2. The processing of the personal data

The chapter two of the Act regulates the processing of the personal data. The controller must use personal data legally, observe the diligence and good data processing, the processing is illegal if it violates the data subjects private life. According to the Article 6 the processing of personal data must be reasonably justified; the aim of the processing, where personal data are regularly acquired and to which they are ordinarily disclosed. That information must be defined before the personal data will be collected, in other words, the personal data can be processed only for that purpose.

[26] Korhonen, R. (2003). Perusrekisterit ja tietosuoja. Helsinki: Edita Publishing.
[27] Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa*. Helsinki: Kauppakamari

According to Article 11 processing of sensitive personal data is prohibited. However, there are some exceptional cases, when processing of sensitive data is allowed, for example, if the data subject gives a permission for it, processing of data is for historical or scientific research or for statistical purposes; medical information, which is necessary for the care of the data subject.

3.3. The rights of the data subject

The controller has an obligation to inform the data subject, when collecting personal data. The data subject has the right to inspect the information about himself. The data subject also has the right to demand correction of incorrect information and to prohibit the processing of his or her personal data for direct marketing, distance selling and opinion and market research, as well as genealogy and personal identity.[28]

The Finnish Data Protection Act also includes right of refusal. According to Article 30, the data subject has the right to deny the controller for processing of information about himself concerning direct mail, distance sales and other direct marketing as well as market and opinion polls, as well as personal identity and genealogy. Also, any person who has knowledge of any other person's characteristics, personal circumstances or financial position in performing the processing of personal data shall not, inform the third party of any such information (professional secrecy).

3.4. Transfer of personal data

According to the section 5 of the Act, personal data can be transferred to the territory of the Member States of the European Union or to the European Economic Area, if the country concerned provides sufficient data protection. When adequacy of the level of data protection, need to take into account the nature of the data, the aim and duration of the processing, the country of origin and the final object, the general and sectoral legal rules in force in the country concerned, the code of conduct and the security measures to be followed.[29]

[28] Vanto, J. (2011). *Henkilötietolaki käytännössä*. s.46-47.
[29] Pitkänen, O., Tiilikka, P., Warma, E. (2013). *Henkilötietojen suoja. S.181*

Personal data can also be transferred to the territory of the Member States of the European Union or to the European Economic Area, if the Commission has made a decision, that a third country or a particular region or sector in a third country or a particular international organization provides a sufficient level of data protection and thus ensures legal certainty and consistency (Article 22 (a)).

If the data subject gives a permission to transfer his/her personal data, it is necessary, that the transfer protects the data subject's vital interest; the transfer is necessary or required by law to safeguard an important for public interest or to create, present, defend or resolve legal proceedings and if the transfer complies with European Union legislation. If some of these vital interests are met the transfer is legal.

3.5. Control of personal data processing

The section 9 of the Finnish Data Protection Act regulates control of personal data processing. The Data Protection Supervisor provides guidance and advice on the processing of personal data. The supervisor also monitors the processing of personal data in order to implement the objectives of this Act and exercises the power of decision as provided in this Act. The data protection authorities cooperate with the data protection authorities of the other Member States of the European Union and, where necessary, provide official assistance (Article 38).

The Data Protection Supervisor is entitled to obtain the information on the personal data processing and any information necessary for the lawfulness of the processing of personal data, without prejudice to the confidentiality provisions, and the right to inspect the personal registers and to use experts in the audit. The Data Protection Board has a similar right in its cases.

3.6. The consequences of abuse

The Personal Data Act also provides for the liability for damages resulting from the unlawful processing of personal data. The Personal Data Act and the Penal Code contain sanctions against violation of the Personal Data Act. The protection of registered privacy and the protection of their interests and rights is not a separate obligation, but is an integral part of the operational objectives.

Based on the Article 47, the controller shall be liable for any financial and other damages incurred by the data subject or any other person against the processing of personal data against this Act.

The penalties are (Article 48):
Any intentional or gross negligence in violation of this law

1) fails to comply with the provisions on the definition of the purpose of the processing of personal data, the filing of a registration report, processing of data, informing, correcting the information contained in the personal register, the denial of the registered right or the notification to the Data Protection Officer,

2) give data protection authorities a false or misleading information on the processing of personal data,

3) Violates the provisions on the protection of personal data and the destruction of personal data;

and thus endangers the protection of the data subject's privacy or his / her rights, he / she shall be sentenced, unless the act is subject to a more stringent punishment stipulated by law, to a fine.

Punishment of violating the Data Protection Act is also regulated in Chapter 38, Articles 1, 2, 8 and 9 of Finnish Penal Code. According to those Articles, the violation of the Personal Data Act is punishable by a fine or up to two years of imprisonment.

4. THE REQUIREMENTS OF THE REGULATION 2016/679 COMPARING TO THE FINNISH PERSONAL DATA ACT

In February 2016, the Finnish Ministry of Justice set up a working group, whose main task was to prepare a legislative proposal on the use of this margin and prepare a proposal for a national supervisory authority. The task of the working group was to evaluate the need for a general law such as the Personal Data Act and to make a proposal for a possible general law.[30]

It is possible and even probable, that the Personal Data Act (22.4.1999/523) will be repealed and provided by the new Data Protection Act, because current Finnish legislation is in conflict with the GDPR and does not respond enough to the digital technology. It seems, that the legislation is not comprehensive and detailed enough. The new legislation will clarify and supplement the Personal Data Act, and therefore it will be more accurate.

The General Data Protection Regulation is directly applicable nationally. However, the General Data Protection Regulation gives to the Member States so-called margin of maneuver. Under the General Data Protection Regulation, it is possible to adopt or maintain national legislation to clarify the provisions of the Regulation. Moreover, national legislation may, in some circumstances, deviate from the obligations of the general data protection regulation.

4.1 Sections that need change and how they need to be changed

The purpose of the Finnish Personal Data Act is to provide for the protection of privacy and other fundamental rights, protecting personal privacy when processing personal data and to promote the development and observance of good data processing. In turn, the aim of the General Data Protection Regulation is to protect fundamental rights and freedoms more generally, not only to safeguard persons right to privacy in the processing of personal data. The GDPR lays down rules for the protection of natural persons in the processing of personal data and rules on the free movement of personal data. The Regulation protects the fundamental rights and freedoms of natural persons, in particular their right to protection of personal data.

[30] Nurmi, P., Talus, A., Jaatinen, T., Hänninen, A., Rantalankila, L., Vettenranta, L. (2017). *EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö*

Personal data must be handled at all stages of the process, starting with data collection and destruction of data in accordance with the security requires. The handling of security requires, for example, the ability to ensure the continued confidentiality, integrity, usability and fault tolerance of systems and services, as well as the ability to recover access to and access to information quickly in the event of physical or technical failure.

4.1.1 Processing of personal data

The Article 6 of the Regulation regulates the Lawfulness of processing. In Finnish legislation the legal basis for the processing has not been written as such, instead, it is more detailed in the Personal Data Act. For example, the Data Protection Board has been able to authorize the processing of personal data in order to carry out a legitimate interest of a registrar or a third party receiving the information. However, because of the Regulation, powers of the Data Protection Board will not be the same anymore. Therefore, in the future, the controller needs to be able to show to the data subject the purpose of collecting personal data and what are the reasons that the personal data will be processed and get his/her permission to it.

According to the Regulation " *In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject.*[31]" Also, if personal data are processed on the basis of consenting, attention should be paid to how consent is requested. Based on to the Regulation, consent must be given explicitly by means of a consent act, such as a written, electronic or oral statement.

According to the Article 28 of the Regulation "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."* Data processing outsourcing regulations will be refined. The processor may not use the services of another personal data processor without the written permission of the controller.

[31]Regulation (EU) 2016/679

The regulation obliges the controller to take measures to protect the rights and freedoms of the data subject and the legitimate interests of the data subject. According to the Regulation, the data subject has the right to at least require that the data will be processed by a natural person on instead of the controller, and tell their views and possibly challenge the decision. Automated decisions and profiling may not be based on specific personal data groups. However, automated decisions based on special categories of personal data are permitted in certain exceptional situations.

Finland should clarify the act by adding an Article, which would regulate the lawfulness of processing. The new Article should contain provisions, that show the legality of processing for example in case of person's position, duties and their treatment in the public sector, in the business or in the organization. The purpose of the processing should be in the public interest.

4.1.2 The rights of the data subject

The Regulation provides for new rights of the data subject. The processes related to the realization of the rights also change somewhat because of the Regulation. The Data Protection Regulation emphasizes the transparency of the processing of personal data and provides more detailed rules on the implementation of the data controller's duty to inform the data subject and the rights of the data subject. To the Finnish legislation should also be added, that the controller should send the processed data to the data subject, tightly presented, transparent, easily understandable and accessible form.

The Regulation also sets deadlines for information and measures taken on the basis of a request from a data subject. According to the Regulation, information on the measures taken following a request from a data subject should be issued without undue delay and no later than one month after the receipt of the request. These time limits need to add to the Finnish data protection act.

Under this Regulation, the data subject has right to obtain a copy of personal data from the controller, but the Finnish legislation does not regulate the form. According to the Regulation if the data subject request for a personal data electronically, the controller shall provide the information in a commonly used electronic form, unless otherwise requested by the registrar.

The Data Protection Regulation gives the data subject with certain exceptions the right to rectify the data and to remove the right to information, ie the so-called right to be forgotten. Similar rights are also included in the Personal Data Act, although the right to be forgotten is not explicitly included in the Act. The obligation to inform the person to whom the data controller has handed over or from whom the data controller has received personal data, is also already regulated in the Finnish Personal Data Act.

According to the Regulation, there are four different situations in which the data subject has the right to restricts the processing of data. The restrictions of the processing of personal data should be should be explicitly stated in legislation so that, after the data subjects restrict, the personal data no longer be subject to processing.

The Finnish Data Act does not regulate the processing of child's data. Because of the Article 8 of the Regulation, Finland should add a new Article to the Act, which would regulate the processing of personal data in case that the data subject is more than 13 years but less than 16 years. There also need to be mention, who is legitimate to give permission for the processing of personal data.

4.1.3 Personal information security breaches

As a new aspect, According to the Article 34 of the Data Protection Regulation, it provides for the controller's obligation to report personal data breaches to the data protection authority and to the data subject. This means that the controller must report the infringement to the supervisory authority as far as possible within 72 hours of the occurrence of the violation. The controller does no need to inform a security breach, if the violation is unlikely to cause the risk to the rights and risks of natural persons. The processor, in turn, must report the security breaches to the controller without undue delay upon receipt of the violation. The notification to the data subject must describe in a clear and simple language, among other things, the nature of the personal data breach and the probable consequences of the security breach.

In case of breaches, Article 83 of the Regulation, regulates General conditions governing the imposition of administrative fines. Those provisions should be added to the Finnish Act on the enforcement of fines (672/2002).

4.1.4 The position and tasks of the Data Protection Officer

According to the Regulation, it is intended to clarify a little the Finnish legislation. The Data Protection Supervisor needs to change to a Data Protection Officer[32]. Basically, the Supervisor's job description will not change; the title will be different and there will be more employees at the Data Protection Office. However, the division of tasks between the Data Protection Officer and the Assistant Supervisor shall be laid down in the Rules of Procedure of the Data Protection Office. The Data Protection Agency shall also have officials and other staff, who would work as rapporteurs.

The Data Protection Officer should have knowledge about personal data protection and have the necessary personal qualities. The Officer and the Assistant Supervisor are also required to have management skills and ability to perform international tasks. The term of the officer is time-limited; it can last only five years, but the same person is able to work two terms in succession.

4.2. Analysis of the requirements of the GDPR

According to the research, the Regulation will change the Finnish Personal Data Act. The data subject's rights and the processing of the data will clarify the most. A major reason for the changes was, that the current Directive did not respond to the issues of globalization and technological development. The Finnish Data Protection Act needs a couple of new sections, but mostly it was only about clarifying the old Act.

Basically, under the new regulation, a data subject has the right to access to the information, what companies have stored for him. Individuals have also more power to affect, how companies use that information. In addition, with a few exceptions, registered persons have the right to be forgotten. This means that registered people may required companies to remove their personal data from companies databases and systems.

According to the new Data Protection Regulation, companies must be able to demonstrate that they handle personal data in accordance with the regulation. Companies need to be able to prove

[32] Hanninen, M., Laine, E., Rantala, K., Rusi, M., Varhela, M. (2017). *Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset.*

that for the processing and storage of personal data is a legitimate reason, personal information is up-to-date, if necessary a person can safely look at the information, that is stored of him and at the request of a person, stored data can be removed from any system.

All this means that it becomes even more important to clarify processes related to customer data processing and to ensure timely information. One of the common challenges for many companies may be that if customer information is scattered across many different systems, removing and retrieving may be quite difficult, inefficient and time-consuming[33]. However, it seems, that the Regulation is important for the future and the changes might have a positive impact on the trust between the parties.

6. CONCLUSION

The aim of the of the paper was to examine the impact of the new General Data Protection Regulation to the Finnish Personal Data Act. The hypothesis of the research was, that the new Data Protection Regulation will change the Finnish Personal Data Act. At the starting point it was not clear how wide the possible change would be. The research would sort out should the Finnish Data Protection only be clarified or should there be added new sections. When the research progressed, also the hypothesis strengthened.

The right to data protection in the European Union is currently regulated in the Directive 95/46/EC. The globalization of the world and technological development have made the data protection very questioned; for example sharing and collecting personal data was a lot of easier and therefore also an abuse of the information increased. In Spring 2016 the Council of the European Union and the European Parliament adopted the General Data Protection Regulation (GDPR), which will enter into force on 25th of May 2018. the General Data Protection Regulation has five goals; more rights for citizens, new obligations for the controller, wider powers to the authorities, strong, unified and comprehensive data protection for the European Union and to develop an internal digital market.

[33] Oprysh, L. (2016). The Forthcoming General Data Protection Regulation in the EU. *Juridica International*, Vol. 24. P.23

The new Regulation will increase the transparency of the processing of personal data. However, the processing should still be legitimate and appropriate and specific purposes of handling personal data should be always determined and reported to the data subject. According to Article 6 of the Regulation, the processing is legitimate without data subject's permission, when it is necessary to protect the interests of a registered or another natural person. Thought, the personal data should still only be processed for the purpose intended and it is illegal to retain the data without purpose. The Finnish Data Act meets these part of the requirements quite well, only the lawfulness of processing needs to be clarified.

The section three of the Regulation regulates the rights of the data subject. The regulation gives more rights to the data subject. Data subject is able to effect to his personal data, for example the controller shall provide to the data subject the aim of processing of the personal data in easily understandable and accessible form, data subject has right ,with certain exceptions, to rectify the data and to remove the right to information, ie the so-called right to be forgotten. The biggest change of this part regarding to the Finnish legislation will be the section, which regulates the processing of child's data. Finland should add a new Article, which would regulate the processing of personal data in case that the data subject is more than 13 years but less than 16 years and also a mention, who is therefore, legitimate to give permission for the professing of childs's personal data.

Because of the international trade and cooperation cross-border transfers of personal data to third countries, to international organizations and back to the Union have increased. Therefore, the regulation includes a part, what states that the transfer may be legal only if the controller and the processor acting in accordance with the regulation. The international organization needs to provide a sufficient level of data protection, which ensures legal certainty and consistency, after that the transfer follows the requirements of the GDPR. However these requirements are already part of the Finnish personal data act.

GDPR also provides for the controller's obligation to report personal data breaches to the data protection authority and to the data subject over a certain period of time. However, informing a security breach is not necessary, if the violation is unlikely to cause the risk to the rights and risks of natural persons. The notification to the data subject must describe in a clear and simple

language, inter alia, the nature of the personal data breach and the probable consequences of the security breach. That should be added to the Finnish Act on the enforcement of fines (672/2002).

According to the conclusion of the research, the hypothesis was pretty much right. Most of the sections need only be clarified. However, it was quite interesting and surprising, that the information of security breaches was not regulated in the Finnish legislation and therefore need to be added to it. All in all, the research showed how important and necessary the General Data Protection Right is for the future.

SOURCES

Books

1. Craig, P. de Burca, G. (2015). *EU Law: text, cases, and materials, sixth edition.* United Kingdom: Oxford University Press.

2. Biondi, A., Eeckhout, P., Ripley, S. (2012). *EU after Lisbon*. Oxford; New York: Oxford University Press.

3. Steiner, J., Twigg-Flesner, C., Woods, L. (2006). *EU Law, 9th edition*. United Kingdom: Oxford University Press.

4. Craig, P. de Burca, G. (2011). *The evolution of EU Law*. Oxford; New York : Oxford University Press.

5. Letsas, G. (2007). *A theory of interpretation of the European Convention on Human Rights.* Oxford: Oxford University Press.

6. Finch, V., McGroarty, J. (2010). *Human Rights.* Dundee: Edinburgh University Press.

7. Pitkänen, O., Tiilikka, P., Warma, E. (2013). *Henkilötietojen suoja.* Helsinki: Alma Talent. (Personal data protection.)

8. Vanto, J. (2011). *Henkilötietolaki käytännössä*. Helsinki: WSOYpro. (The Personal Data Act in Practice.)

9. Voigt, P., Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Switzerland: Springer International Publishing

10. Gutwirth, S., Leenes, R., Hert, P. (2015). *Reforming European data protection law.* Dordrecht: Springer.

11. Hanninen, M., Laine, E., Rantala, K., Rusi, M., Varhela, M. (2017). *Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset.* Helsinki: Helsingin Kamari Oy. (Processing of personal data: requirements of the EU Data Protection Regulation)

12. Korhonen, R. (2003). Perusrekisterit ja tietosuoja. Helsinki: Edita Publishing. (Basic registers and data protection)

13. Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa*. Helsinki: Kauppakamari
(Protection of identity in Finland)

Articles

14. Vataman, D. (2010). Lex ET Scientia International Journal. *History of the European Union,* Vol. 17, Issue 2), 107-137

15. Robinson, W. (2010). Manuals for Drafting European Union Legislation. *Legisprudence*, Vol 4, Issue 2, 129-156.

16. Frost, W L. (2000). The Developing Human Rights Discourse: A History of the Human Rights Movement. *Trinity Law Review*, Vol 10, 1-28.

17. Van der Vyver. (1979). The Concept of Human Rights: Its History, Contents and Meaning. *Acta Juridica*, Vol 1979, 10-32.

18. Douglas-Scott, S. (2011). The European Union and Human Rights after the Treaty of Lisbon. *Human Rights Law Review*, Vol 11, Issue 4, 645-682.

19. Lambert, S., Lindsay-Strugo, A. (2008) Focus on Article 8 ECHR:Recent Developments. *Judicial Review*, Vol. 13, Issue 1, 29-40

20. Albrecht, J. P. (2016). How The GDPR Will Change The World. *European Data Protection Law Review*. Vol. 2, Issue 3, 287-289.

21. Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, Vol. 47, Issue 3, 809-848.

22. Ferretti, F. (2016). The Foundations of EU Data Protection Law. *European Data Protection Law Review (EDPL)*, Vol. 2, Issue 2, 278-280.

23. Oprysh, L. (2016). The Forthcoming General Data Protection Regulation in the EU. *Juridica International*, Vol. 24, 23-31.

24. Blume, P. (2015). The Data Subject. *European Data Protection Law Review*, Vol. 1, Issue 4, 258-264.

25. Reijneveld, M. (2017). A Journal of Law, Technology and Society. *Quantified Self, Freedom and the GDPR.* Vol. 14, Issue 2, 285-325

26. Goldberger, D., Akerman, N., Levin, J., Ray, D. (2017). Cross-Border Data Privacy Issues. *Cardozo Journal of International and Comparative Law*, Vol 25, Issue 2, 379-vii.

27. Allisom, S. (2009). The concept of Personal Data under the Data Protection Regime. Edinburgh Student Law Review, Vol 1, Issue 1, 48-65

Legal Acts

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

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)

Henkilötietolaki. 22.4.1999/523. (Finnish Data Protection Act)

Rikoslaki. 19.12.1889/39. (Finnish Penal Code)

Others

Finnish Ministry of Justice (2017): *Implementation of the EU Data Protection Directive OM005: 00/2017 LEGAL PREPARATION*

Nurmi, P., Talus, A., Jaatinen, T., Hänninen, A., Rantalankila, L., Vettenranta, L. (2017). *EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö.* Helsinki: Lönnberg Print & Promo, Oikeusministeriö. (Report of the Implementation Working Party of the EU General Data Protection Regulation)

Talus, A., Autio, E., Hänninen, A., Pihamaa, H. T., Kantonen, S. (2017). *Miten valmistautua EU:n tietosuoja-asetukseen*? Helsinki: Oikeusministeriö. (How to prepare for the GDPR?)