PROTECTION OF PERSONAL DATA AND PRIVACY IN BANKING SECTOR IN KOSOVO AND ITS IMPACT IN CONSUMER PROTECTION

PhD. student **Fitim GASHI**[1]
Professor **Bedri PECI**[2]

Abstract

Following the national and EU legal framework, protection of personal data and privacy includes almost all type of business including the banking sector. Kosovo as a new state is trying to build a legal system which aims to be in compliance with the EU legal framework also in area of personal data and privacy and in the meantime in compliance with consumer protection rules. Taking into consideration that Kosovo recently established the National Agency for Protection of Personal Data while banks are dealing with big data, customers are faced with the situation where their data can be not treated as law requires. The protection of personal data is a fundamental right and banks deal with personal data in daily basis. We also may know that banks are obliged to receive personal data but the main challenge remains the protection of customer data and privacy. The aim of this paper is to raise the issue of protection of personal data and privacy in banking sector as the banks receive and handle personal data in a daily basis. On this paper we will see how the protection of personal data is regulated and how banks are obliged to protect personal data and customer privacy in Kosovo and how it has impact in the consumer protection in banking sector.

Keywords*: privacy, personal data, consumer protection, bank.*

JEL Classification: K23, K36, K38

1. Protection of privacy in banking sector in Kosovo as a way of consumer protection

1.1 The concept of personal data protection

The protection of personal data is a fundamental right in Kosovo which is guaranteed by the Constitution of the Republic of Kosovo. Constitution specifies that privacy and family life, inviolability of residence, confidentiality of correspondence, communications by telephone and with other equipment and protection of personal data are guaranteed to each citizen (Kosovo Constitution 2008: Article36). Therefore, the Constitution and the Law also guarantee the implementation of some of the major international and European data protection conventions[3]. These conventions are: Universal Declaration of Human Rights (Article 12)[4]; European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8)[5]; Convention 108/EC and Additional Protocols[6]; EU Directives 2016/279[7] and Directive 2006/24/EC and its Protocols[8]; The international Covenant on Civil and Political Rights (Article 17)[9]; the Charter of Fundamental Rights of the EU (Article 7)[10] and the Treaty of Lisbon[11] (Article 16).

Thus, the protection of personal data is enshrined in these powerful international instruments

---

[1] Fitim Gashi – Faculty of Law, Financial Law Department, University of Pristina, Kosovo, fitimigashi@mail.com.
[2] Bedri Peci – Faculty of Law & Chief of Financial Law Department, University of Pristina, Kosovo, bedri.peci@uni-pr.edu.
[3] Constitution of the Republic of Kosovo, article 22- Directly Implementation of International Agreements and Instruments.
[4] Universal Declaration of Human Rights, 10 December 1948.
[5] European Convention for Protection of Human Rights and Fundamental Freedoms, 4 November 1950.
[6] 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).
[7] Regulations(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).
[8] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[9] International Covenant on Civil and Political Rights – by the General Assembly resolution 2200A(XXI) of the 16 December 1996, entry into force 23 March 1976.
[10] Charter of the Fundamental Rights of the European Union (2000/C364/01).
[11] Treaty of Lisbon – amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.

which have placed this right at a very high level of the international justice. As Bygrave notes, formally, data privacy law is aimed primarily at safeguarding certain interest and rights of individuals in their role as data subject- that is when data about them is processed by others. These interests and rights are usually expressed in terms of privacy, and sometime in terms of autonomy or integrity.[12]

The issue of personal data protection continues to be subject of discussion among scholars and policymakers. The reason it is still part of the debate is related to the inadequacy of its affirmation as a fundamental right. The right to protect personal data is not intended to hinder the processing of data, on contrary, it seeks to ensure their free movement as well as to protect individuals from an unauthorized collection, shortage and dissemination of personal data. For this reason, the right to protect personal data is often found in conflict-laden scenarios where on one hand the right of a person to own his information stands and on the other hand there is a serious risk of its infringement.

Among the main pillars of the EU, such as the European Community, the Common Foreign and Security Policy, a very important pillar is also the Justice and Home Affairs Cooperation which is considered as the third pillar and which also includes the protection of personal data and privacy or called as "privacy"[13]

In order to harmonize this problematic issue to a new level, the EU has approved a new regulation known as GDPR[14] (General Data Protection Regulation) which aims to bring the privacy to a new stage.

The protection of European citizens' data is dominantly present in the GDPR and is not restricted to European companies or countries. All companies that process European citizens' personal information must comply with the new regulation. For example, technology companies from United States must also adhere to this regulation even though their customer data will not reside in a European data center, or the company is based outside Europe.

Despite the fact that the research field of data protection has seen significant developments in recent years, this area remains an unexplored area and leaves the door opened for further research and analysis. Its dynamic nature constantly demands response and the need of new legal framework developments. Therefore, we need to consider how data protection rules should be applied to different sectors including banking sector. We live in a time of rapid developments of technology and digitalization of banking services and at the same time, these developments have enabled the rapid collection of big personal data from bank customers. However, the gathering of a large number of data, requires the implementation of safe measures. Thus, the protection and proper handling of personal data in the banking sector is a challenge. The protection of personal data is a hot topic also in the EU banking sector where various organizations within the area have initiated new laws and regulations to protect them. One of the sectors affected by these regulations is the banking sector, which data are known as financial data in EU and there is a number of legal instrument at place that regulate the protection of financial data.[15] Although financial data are not considered as sensitive data under Convention 108 or under the Directive on the Protection of Personal Data, measures must be taken in their processing to ensure their accuracy and security "privacy by conception" (privacy by design). On the other hand, information is a powerful weapon

[12] Lee A. Bygrave, *"Data Privacy Law" an international perspective*, Oxford University Press, UK, 2014, fq 6.
[13] Dr. Marko Bello, *E Drejta Institucionale Komunitare Europiane*", Tirane, 2010, p. 291.
[14] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html (accessed on January 5, 2020).
[15] a) Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004, on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC; b) Regulation EU no.648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivates, central counterparties and trade repositories; c) Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies – article 36; d) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC - Article 3; e) Recommendation No. R(90) 19 of the Committee of Ministers to Member States on the Protection of Personal Data used for Payment and Other Related operations, Council of Europe, 13 September 1990.

in economy and various companies including banks collect personal information of their clients for business purposes on daily basis.

2. Legal obligation of banks in Kosovo to protect personal data and customer privacy

Banks are obliged to maintain confidentiality about their business relationships with customers and about their customers' accounts; they must preserve banking secrecy or the "banking secret".[16]

The Constitution of the Republic of Kosovo (hereinafter CRC) ensures that each person holds the right to the protection of personal data (Article 36, paragraph 4). Whereas, in the second sentence of this paragraph it is stipulated that the collection, storage, correction and use of personal data about a person can be done only as regulated by law. A special law which is considered a Lex Specialis in the field of protection and processing of personal data in Kosovo is Law No.06/L-082 on Protection of Personal Data (hereinafter LPPD)[17] which sets forth the rights, responsibilities, principles and measures relating to the protection of personal data which the law repeals the prior law of 2010 (03/L-172).

Pursuant to Article 2, paragraph 1, subpar.1.1 of LPPD "Personal Data - any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

By law, personal data may be processed by any natural or legal person from the public or private sector who processes personal data for and on the account of the data controller-Article 1, par.1.15 of the LPPD. The private sector controller can be a financial institution, for example, commercial banks that have personal data related to civil, financial, employment, customer housing and other data or any changes that occur in these relationships.

Whereas, the National Agency for Personal Data Protection (NAPDP) is an independent state institution, established under LPPD and is responsible for overseeing the lawfulness of personal data processing. The Agency's obligation is to establish new bylaws and prepare them for approval after the appointment of the Commissioner. According to the article 29, par.2 the agency advises public and private bodies on data protection issues, decides on data subject complaints, conducts inspections and audits, informs the public on data protection issues and development and promotes the fundamental right of personal data protection.

In addition to the law (LPPD), commercial banks in Kosovo are required to implement a series of other legal instruments that oblige them to collect and process their client's personal data such as: Law on Banks, Microfinance Institutions and Non-bank Financial Institutions[18],Law on the Prevention of Money Laundering and Combating Terrorist Financing[19] which obliges commercial banks to collet personal data, Law on Payment System[20], Law on Labour[21] , Law on Enforcement Procedure[22] and other laws that are applicable in banking sector.

The basic principles of data protection that financial institutions and other legal entities that process personal data must abide by are: personal data must be processed legally and in accordance with the law; to be collected for concrete, clear defined purposes by law and to be processed in a

[16] Peter Koslowski, *The Ethics of Banking, Conclusions from the Financial Crisis*, Springer Science+Business Media B.V. 2011, p. 105.
[17] Law No. 06/L-082 on Protection of Personal Data, by Assembly of the Republic of Kosovo, 30 January 2019.
[18] Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions - Article 52, 12 April 2012.
[19] Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing – Article 19 customer due diligence, Article 20- record keeping.
[20] Law No. 04/L-155 on Payment System – Article 27 Information on individual payment transactions and issuance of receipts, Article 52-Privacy, 04 April 2013.
[21] Law No. 03/L-212 on Labour, Article 11-The content of an Employment Contract, 01 November 2010.
[22] Law No. 04/L-139 on Enforcement Procedure- Article 155 Obligation to provide data on the account.

manner consistent with those purposes; be relevant, respective and not enormous in relation to the purpose for which they are collected and processed; be accurate, complete and where necessary updated, appropriate measures must be taken to erase or correct inaccurate or partial data, taking into account the purposes for which it is collected or processed and stored in a form that enables the identification of the subject of personal data but not longer than necessary to fulfill the purposes for which this data is collected for the further processing .[23]

Not adhering by these principles often leads to unauthorized and illegal processing of personal data, which can cause serious breach of customer privacy.

According to LPPD any person who considers that his/her right to privacy has been violated in terms of personal data may issue a complaint to the National Agency for Personal Data Protection. Citizens of the Republic of Kosovo [24]have raised concerns mainly about the processing of personal data by controllers, data processing for direct marketing purposes, unauthorized disclosure of data, unauthorized disclosure of sensitive data, biometric data processing, data processing without consent, processing of personal data through social networks as well as processing of inaccurate data. These complaints have been mainly directed at central and local institutions, banking sector, microfinance sector, insurance companies, health sector, shopping malls, etc.

Data privacy refers to who's enabled access to costumer's information provided to institutions with whom they've entered into a business relationship. Workers at banks need certain information to verify the identity of those accessing a client's account. Problems arise with data security when employees, security officials and others tasked with the protection of sensitive information fail to provide adequate protocols. They may act carelessly and leave their credentials around at home or in public places. This lapse brings consequences in regard of costumer's data protection.

Banking secrecy includes the duty of confidentiality toward the customer and the bank's right to refuse information to third parties, including a country's tax authorities, about its customers[25]

The same exists in most countries. It derives from the civil contract law and is a product of contractual freedom. It does not derive directly from the constitutional principle of human dignity since it is not person-related but property-related,2 although it belongs to the rights of personality that deserve legal protection to prevent infringement of personal rights or invasion of the private sphere[26], including the banking sector.

3. Financial data as part of personal data and their protection in Kosovo

Financial data is all the personal information on incomes, expenses, deposits and loans that a person has but that are not categorized as sensitive data. Financial data are very important for all banks institutions as this information enable them to target certain clientele. Also, these data serve for the financial capacity to be analyzed carefully by banks when they are about to approve a loan or other banking products.

For the purpose of collection of the secured financial information, Central Bank of the Republic of Kosovo (CBK) according to its duties and responsibilities[27] has created the Credit Register of Kosovo (CRK), which is a system that collects information of all Kosovo residents about loans, credit cards, overdrafts and other credit products, including information on debt payments. In addition, all financial institutions licensed by CBK must be members and reporters to

[23] These principles can be found in detail in Article 12- Principles of Processing of Personal Data in LPPD.
[24] For more details refer to the article 52 of LPPD.
[25] Cf. Dieter Cahl, Joachim Klos, *Bankgeheimnis und Quellensteuer im Vergleich internationaler Finanzmärkte* [Banking secrecy and witholding tax, comparing international finance markets], Herne/Berlin (Neue Wirtschaftsbriefe) 1993, p. 5.
[26] Cf. F. Beutter, *Geheimniscarakter des Geldes und ethische Grundlagen der Geheimhaltungspflicht*, „Acta Monetaria", 2(1978), p. 15 (own trans.): "In the measure in which money, e.g. as remuneration for work done, has a close relation with the human person".
[27] Law no. 03/L-209 on Central Bank of the Republic of Kosovo - Article 8 par.1.2.

the CRK. For more, all financial institutions must consult information within CRK system during the lending process. CRK identifies the subject of data of personal and business entities and their debt obligations towards financial institutions operating in Kosovo. The role of these entities can be as following: borrower, co-borrower, guarantor, shareholders and directors of the legal entity to which the credit obligation is issued. All borrowers and other included in bank product maintain their right to data privacy in accordance with the law.

Therefore, the credit report is an important document which shows both positive and negative information on the credit history of each person included in the banking product and this information is critical during the lending process of all financial institution because they must respect the categorized conditions.

Credit Report Content. The credit report provides information on personal data about current loans, credit history as well as data related to credit obligations. All information reported to the CRK is confidential and based on the applicable legislation and regulation, which is maintained in the CRK database. The information presented in the report, including the information on personal loans and the information in which the borrower has the role of a related person, will appear in the credit report at least 5(five) years after the loan has been fully paid.[28]

3.1. Role of Credit Report

When applying for a loan, the Credit Report along with other relevant factors such as the financial status, ability to pay on time as well as opportunities to secure the loan through collateral (mortgage) present concrete data that may affect the approval or rejection of the loan application by the lending institution. Moreover, all financial institutions are required to report to the credit register on time.

3.1.1. Disputing the data on credit report

For any remarks on the data presented in his/her credit report, the borrower must fill in a form stating the disputed data and address it to the institution that reported this data. The institution will process this complaint and respond in writing form within 5(five) days. This data can only be corrected after being verified on the basis of various documents provided by the borrower which prove that the actual data in his/her report are incorrect. After this decision, the borrower must confirm his/her agreement or disagreement with the decision taken by the respective institution. If the borrower disagrees with the decision reached by the reporting institution, he/she may refer to the "Complaint and Financial Services Users Division" at the CBK. The decision on the borrower's appeal should be taken within ten (10) business days. In case where the Complaint Division certifies that the disputed data in the report are correct but the party does not agree with the decision taken, then the party may refer the matter to the relevant legal authorities for the resolution of the dispute.

4. The importance of consent in the protection of personal data in banking sector

For many reasons, state institutions can and should regulate the purposes for collection of information and their use for solely the purposes for which they were collected. To accomplish this mission, this arrangement of regulation must include some very sensitive sectors such as personal data related to health, financial and children.[29]

Consent of the Data Subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies consent to the processing of personal data relating to him or her.[30] Consent is a

[28] Regulation on Credit Registry, Article-5 Permissible, CBK 24 February 2012.
[29] Paul H. Rubin & Thomas M. Lenard, *Privacy and the Commercial Use of the Personal Information*, Springer Science&Business Media, NY, 2002, p. 3.
[30] LPPD, Article 3, par.1.17.

document in the form of a statement that the bank's client agrees to authorize the bank to access its financial records in the credit history, to process the data for direct marketing and other purposes under the bank's privacy policies. So, by signing this document the client agrees to share his financial privacy and agrees to accept online marketing from the bank in the future.

Moreover, consent is a statement served by the bank in "take it or leave it" form, and thus the client is obliged to share some privacy without having the opportunity to negotiate. The risk is that clients are forced to agree to the services the financial institution offers to exchange their data and thus to overcome the purpose of personal data collection.[31]

But the situation changes when it comes to daily business where the banking officers complete the consent mostly to fulfill a legal requirement and the customer signs it without been informed by the bank officer. In this situation, the customer signs the consent blindly.

A solution to this problem has been provided by the GDPR, according to which a service provider that may also be a bank institution, may not condition the provision of the service with consent-giving when it is not required in order to provide that service. So, this aims to stop banks from using personal data to make their bid using the situation with the consumer.[32] The GDPR regulation is applicable to all companies doing business with any citizen of the EU and this has enforced the customer rights in a new level, so the companies need to be careful about containing clear consent to use information for different types of activities.

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including electronic means, or an oral statement.[33]

Consent should contain: a) name of the person giving the consent; b) date when the consent was given, the statement of privacy policy by institution at the time consent was granted, c) any documents or data forms containing information provided by the consenting party. The LPPD nor the GDPR don't outline specific requirements for how long consent is considered valid. It's a good idea to refresh consent periodically, particularly when you make changes in your company's data guidelines.

4.1. Withdrawing consent

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of the processing of data based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.[34] The right of withdrawing of consent is guaranteed also with Kosovo laws, (LPPD article 6 par.3, article 12, par.2.3, article 12, par.2.4) Any requests made by consumers to take back any permissions granted regarding their data should be handled quickly and efficiently. Banks should establish a clear process for withdrawing consent and documenting every step of the process. Systems should be updated to reflect the customer's request and immediately block access to this data. Everything should be timed to prevent the inadvertent passing of protected information once companies no longer have clear consent to use that information.

In sum, for the data banking world, the question is not whether but how consent can be implemented within data protection. Problematizing consent in terms of power asymmetries is linked to the discourse of data protection rules, which stresses data subjects' dependence on digital banking platforms, and for that reason, calls into question whether data protection can continue to rely on consent. It, however, fails to provide a coherent narrative articulating why power asymmetries are problematic. The fact that consent, when given in situations of factual dependency,

[31] https://ec.europa.eu/info/sites/info/files/file_import/1606-big-data-on-financial-services_en_0.pdf (accessed on January 5, 2020).
[32] GDPR par. 32, 68, Article -7 par. 1, 2, 3, 4.
[33] GDPR, par. 32.
[34] GDPR, Article 7, par. 3.

might result in non-compliance with data protection law, does not present a particularly powerful narrative. Highlighting information asymmetries, in contrast, is linked to the popular and intuitive narrative of the banking data. The banking data discourse is supported by an evidence-based approach of reasoning. On the banking data, consumers exchange "their data" in order to benefit from the services provided by the banks.

Banks should not only give the consent form to customers to fulfill a formal obligation but they should inform them what they are signing and if the customer doesn't read it, at least they should explain what the consent contains and why it is obliged by banks.

5. Where do banks stumble in protecting personal data and clients' privacy?

Data protection is pragmatic: it assumes that private and public actors need to be able to use personal information because this is often necessary for societal reasons. Data protection regulation does not protect us from data processing but from unlawful and/or disproportionate data processing[35]

Banks are among the most regulated and supervised institutions for many reasons and above all, because of the functions they perform. In this regard, they are bound by a variety of laws and regulations from various fields including laws and regulations relating to the protection of customer data privacy.

In the day-to-day practice of financial institutions, in particular commercial banks in Kosovo tend to protect and operate with personal data in accordance with the applicable laws and regulations. However, despite this caution, in Kosovo, personal information is leaked and customer privacy is violated. If you visit a branch of any bank, you may notice that there is not enough space to accommodate the customer where the privacy from other customers would be kept in a proper way. So the physical space where the customers are served is not specifically separated for it to enable a normal communication between the client and a bank officer without the conversation being heard by other parties, for example bank employee or customers waiting in the queue. This fact does not make the bank customer feel safe because he himself witnesses his privacy being violated. In addition, the practice of signing documents "blindly" is applied where the bank officers do not clarify to the client that a certain consent is a form of agreement for e.g. for them to receive the latest offers. But then the clients begin to claim when they start to receive e-mails or SMS for the latest bank offers. This wild practice of marketing by banks is frustrating many customers who issue claims, but the same are resolved within the bank and customers are convinced that this is done for their good.

In this regard, CBK, the Agency and the Association of the Banks should sensitize the public to raise all their concerns related to the protection of personal data and privacy in banking sector. No one better than these institutions could be involved in educating and informing the customers about raising concerns to the relevant institutions about data privacy.

The CBK has already a financial literacy as well as a complaint department and these departments should be helped by the management of CBK to play a crucial role in protecting the customer's privacy.

Laws and CBK regulations are mandatory to banks in their daily operating. On the other hand, banks today offer a wide range of banking products and services and in this relationship with customers, banks receive different customer data. As part of the obligations of banks regarding the protection of personal data, based on personal investigation and customer survey I have concluded that:

- Banks obtain the customers consent before entering into a relationship with him/her and at the same time use this consent for access to financial information, making direct marketing, promotion of banking products and offers without informing the client in advance.

- Commercial banks receive more data than necessary, thereby exceeding of adequacy as

[35] P. De Hert and S. Gutwirth "*Reinventing Data Protection*", Springer Science+Business Media B.V. 2009, Belgium.

specified in article 2 of the LPPD

- Lack written documentation regarding customer information on each product/services.
- Lack information regarding the person, the manner and purpose of the data processing and the right of the data subject.

Banks are known as well-organized and consolidated entities in Kosovo. We can now say that there is a worthy competition in the Kosovo banking market in terms of providing banking products and services and at the same time quality competition. This competition should also include how they operate, namely the level of privacy protection, the handling of customer complaints and ultimately customer protection. Undoubtedly, the level of bank customer privacy protection affects the level of bank customer protection since privacy is an individual's fundamental right. Therefore, the relevance of protection of these rights. The level of privacy protection at all levels including the banking sector has evolved in Kosovo, especially with the establishment of the National Agency for the Personal Data Protection, but what needs to be done further is to inform the client about their rights in banking sector related to their privacy. In this context, CBK as a regulator and supervisor of the banking system is expected to use it legal authority to advocate as much as possible in the cause of protection of customer privacy and generally customer protection in banking sector.

In conclusion, information has been critical in function of market economy. It enables innovation and is a primary driver of resource allocation and price discovery in markets. But, information plays a particularly important role in financial services. Indeed, financial products are not physical material goods but constructed from packages of information bound together by legal contracts. If used properly, information can lead to competitive, well-functioning, responsive markets that meet the needs of citizen-consumers more fairly and efficiently. But, if information is not used within a proper framework, it can result in dysfunctional markets, market abuse, and major consumer detriment including social and financial exclusion, discrimination and, in some cases, abuse of fundamental rights.[36]

Bibliography

1. Dieter Cahl, Joachim Klos, *Bankgeheimnis und Quellensteuer im Vergleich internationaler Finanzmärkte [Banking secrecy and witholding tax, comparing international finance markets]*, Herne/Berlin (Neue Wirtschaftsbriefe), 1993.
2. Federico Ferretti, *EU Competition Law, the Consumer Interest and Data Protection*, Brunel University London, 2014.
3. Lee A. Bygrave, *"Data Privacy Law" an international perspective*, Oxford University Press, UK, 2014.
4. Marko Bello, E Drejta, *Institucionale Komunitare Europiane*, Tirane, 2010.
5. P. De Hert and S. Gutwirth, *Reinventing Data Protection*, Springer Science+Business Media B.V. 2009, Belgium.
6. Paul H. Rubin & Thomas M. Lenard, *Privacy and the Commercial Use of the Personal Information*, Springer Science&Business Media, NY, 2002.
7. Peter Koslowski, *The Ethics of Banking, Conclusions from the Financial Crisis*, Springer Science+Business Media B.V. 2011.
8. Universal Declaration of Human Rights, 10 December 1948.
9. European Convention for Protection of Human Rights and Fundamental Freedoms, 4 November 1950.
10. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
11. Charter of the Fundamental Rights of the European Union (2000/C364/01).
12. Treaty of Lisbon – amending the Treaty on European Union and the Treaty estabilishing the European Community, signed at Lisbon, 13 December 2007.
13. Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004, on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC.
14. Regulation EU no.648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivates,

[36] Federico Ferretti, *EU Competition Law, the Consumer Interest and Data Protection*, Brunel University London, 2014.

central counterparties and trade repositories.
15. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.