AMERICAN UNIVERSITY OF ARMENIA
ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ
LL.M. Program
ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

Personal Data Protection: Liabilities of Financial Organizations in Regard with Their Customers

Whether the use of a client's personal data for the reasons other than the intended purpose by financial institutions is lawful under Armenian law where the data was collected for conducting client due diligence based on the "Know Your Customer" principle.

STUDENT'S NAME

TATEVIK KYANDARYAN

SUPERVISOR'S NAME

PROF. NSHAN MATEVOSYAN

NUMBER OF WORDS

11,283

Contents

Introduction

When talking about personal life privacy, we should remember the words of an American business magnate, investor, and media proprietor Steve Jobs: "*Privacy means people know what they're signing up for, in plain language, and repeatedly. I believe people are smart. Some people want to share more than other people do. Ask them.*".

Data protection is the body of law that secures for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, concerning the automatic processing of personal data relating to him.[1] "It is an interesting case of a corpus of transnational law in the sense of legal rules, which develop rapidly and simultaneously in municipal and international law, into a tissue binding together private and public entities across national borders."[2]

Personal data have and will continue to play an important role in an international humanitarian context. Information technology and its applications in data processing are used in the same way in many countries and are developed by a multinational industry. The scarcity of expertise and the desire to avoid unnecessary divergences between national laws have created a need for frequent international consultation.

The right to respect for private life is one of the fundamental human rights, the legal basis of which is ***Article 8 of the European Convention on Human Rights***. It states: "*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others*".

In principle, ***the European Convention on Human Rights*** protects personal information and one can reasonably expect that it will not be published or used without a person's consent.[3] On the

[1] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 1, Jan. 28, 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
[2] Frits W. Hondius, *A Decade of International Data Protection*, 30 Netherlands Intl. L. Rev. (1983).
[3] Council of Europe European Convention on Human Rights, art. 8, September 3, 1953, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

other hand, the protection of personal data cannot be considered an absolute right. It is necessary to ensure a balance between these and other fundamental rights, taking into account the principle of proportionality. The European Court of Human Rights has repeatedly referred to this issue, stating that the protection of personal data plays a fundamental role in the exercise of the right to respect for private life.[4] Nowadays, securing personal data is one of the main concerns of democratic countries.

From 2007 every year on January 28, *"International Data Protection Day*" is celebrated.[5] The holiday is designed to keep users from forgetting to follow online rules of conduct that help to protect their virtual and real lives. The day coincides with the anniversary of signing the Convention for the Protection of Individuals Concerning the Automatic Processing of Personal Data (the Convention) in 1981. The Convention (also called Convention 108) protects the right to privacy of individuals, taking account of the increasing flow across frontiers of personal data undergoing automatic processing. The Convention is the first international binding instrument in the field of personal data protection, which defines the privacy mechanisms for the protection of human rights and defines the concept of "personal data".

European Union (EU) Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (*General Data Protection Regulation (GDPR)*) provides for a harmonization of the legal data protection regime throughout the EU. The European Union has introduced **GDPR** in order to safeguard its citizens by systematizing data privacy laws and mechanisms across industries, regardless of the nature or type of operations. GDPR also aims to empower EU citizens by making them aware of the kind of data held by institutions and their rights to protect their personal information.

Article 8 of the Charter of Fundamental Rights of the European Union states, that "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*"

---

[4] *S. And Marper V. The United Kingdom,* 2008 ECHR 30562/04 and 30566/04, para 103.

[5] Council of Europe, *28 January - Data protection day*, *available at* https://www.coe.int/en/web/portal/28-january-data-protection-day (last visited March 11, 2020).

As part of European civilization and a member of the Council of Europe, the Republic of Armenia **(**hereinafter refers to as RA**)** adopts a policy of protection of personal data based on European standards and principles. Under **the RA Law on Protection of Personal Data**, protection of personal data has been secured by the state; the mutual rights and obligations of private data subjects and developers have been balanced. The law defines the term "personal data" as "any information relating to a natural person, which allows or may allow for direct or indirect identification of a person's identity."[6]

Bankers have always been duty-bound to keep personal information confidential, but there was no corresponding right vested in clients to check the accuracy and relevance of data concerning them. [7] In recent years, financial service providers have begun using and processing different types of data to make financial services and products more cost-efficient and tailored to consumers' needs, thus the need to protect personal data remained particularly relevant.

The relationship between a bank/credit organization and its customers is not strained. Banks and credit organizations are more focused than ever on rebuilding this relationship around trust and loyalty. It is known, that 48 % of customers would lose trust in their bank and 28% would switch to a new bank if their bank were accused of unethical business practices that did not impact them personally[8]. To achieve this objective, financial institutions must meet the customer's expectations and deliver services that are convenient, integrated and accessible.

It should also be emphasized that the banking system plays a crucial role in helping to prevent **money laundering and terrorism financing**. Money laundering would be largely impossible without the network of financial institutions that facilitate it. Both international and national Anti-Money Laundering (AML) regulations impose various strict obligations on banks and other financial organizations, including *customer due diligence[9], verification of clients' beneficial owners[10], reporting of suspicious and unusual transactions[11], and refraining from the execution of transactions*. Thus, banks and other financial organizations must use their internal data and IT systems not just for

---

[6] Republic of Armenia Law on Protection of Personal Data No. HO-49-N, adopted on May 18 2015, Art. 3
[7] Hondius, *supra* at Vol. 30 (2).
[8] World Economic Forum, *"The Appropriate Use of Customer Data in Financial Services" available at* https://www.weforum.org/whitepapers/the-appropriate-use-of-customer-data-in-financial-services (last visited April 19, 2020).
[9] Republic of Armenia Law on Combating Money Laundering and Terrorism Financing No. HO-80-N, adopted on May 26, 2008, Chapter 5.
[10] *Id,* Article 16(5(2)).
[11] *Id,* Article 6.

regular reviews of customers' primary data, but also to perform the ongoing monitoring of transactions. Meanwhile, the AML and anti-corruption regulations, which require a company to conduct due diligence on those entities and individuals they intend to do business with, can create a need to consider the impact of international and local data privacy regulations.

To ensure that financial institutions can detect potential money laundering schemes, there are several legal requirements, which culminate in the customer due diligence procedure, often referred to as the "**Know Your Customer" (KYC)**.

While banks and other financial organizations are no strangers to regulation, adhering to these requires the collection of large amounts of customer data, which is collated and used for various activities. Of the kind mentioned could be a *client or customer onboarding* (the process by which a customer establishes a relationship with the bank and provides all of the necessary information for the bank to open an account), *relationship management, accounting and commercial purposes.* During these processes, customer data is exposed to a large number of different people at different stages.

"Personal data must be stored in such a way as to exclude the identification thereof with the data subject for a period longer than is necessary for achieving predetermined purposes."[12] This is attributable to the fact that banks and other financial organizations often forget, and apply the "Know Your Customer" principle for their benefit, for other risk assessments and direct marketing.

Article 1(2) of the RA law on "***Protection of Personal Data***" states that "[c]haracteristics pertaining to personal data constituting state and official, banking, notarial, insurance secrecy, legal professional privilege, those used in the course of operations concerning national security or defense, **as well as those used in the fight against money laundering and terrorism, operational-intelligence activity and proceedings shall be regulated by other law**s".

Meanwhile, Article 22 of the Republic of Armenia "***Law on Combating Money Laundering and Terrorism Financing***" states that "[r]eporting entities **should maintain** the information (including documents) required under this Law, including the information (documents) obtained in the course of customer due diligence, **regardless of the fact whether the transaction or business relationship is an ongoing one or has been terminated…"**

[12] Republic of Armenia Law on Protection of Personal Data, Art. 5(5).

It was noteworthy, that international AML regulations also require companies to retain personal data long after a business relationship ends. This is in direct tension with GDPR, as **GDPR** mandates that personal data should not be retained "**no longer than is necessary for the purposes for which the personal data are processed.**"[13]

Article 6 of GDPR requires data controllers to establish a legal basis for collecting and processing personal data – including data required for AML purposes. For institutions with AML obligations, the most relevant justifications provided by GDPR are article 6 (c), which allows for the processing of personal data "for compliance with a legal obligation to which the controller is subject" – typically, AML laws or sanctions and article 6(f), which allows for data processing for "legitimate interests", justifiable on a case-by-case basis.

Financial organizations must identify ways to secure personal data that is no longer connected to an existing business relationship but that must be retained for at least several years for AML compliance purposes. At the end, there is a requirement to delete personal data (unless express consent is given to retain that data) or if the data processor is otherwise required to retain the personal data (e.g. for the purposes of court proceedings).

It follows, that many financial organizations can collect and retain their customers' data as a means of countering anti-money laundering, arguing that it is done within the ***Law on Combating Money Laundering and Terrorism Financing***. Thus, it is important to ascertain whether this principle will not further promote the collection and use of customer data for other reasons.

This paper aims to provide a comprehensive analysis of data protection law in the Republic of Armenia and international practices regarding the engagement of state liability for legislative changes. The reasons how banks and financial organizations solicit customer personal information based on the "Know Your Customer" principle required by law will be discussed. This paper will address a very important question of why financial companies should maintain and use their customers' personal data without going beyond the scope of "Know Your Customer" principle. The importance of creating sufficient resources to protect customers' personal data when using online lending will be discussed.

[13] 2016/679 GDPR § 5 (2018 through May 25).

The specific question is ***whether the use of a client's personal data for the reasons other than the intended purpose by financial institutions is lawful under Armenian law where the data was collected for conducting client due diligence based on the "Know Your Customer" principle.***

Thesis paper literature is based on a comprehensive study of the Armenian legal framework specifically on Law on Combating Money Laundering and Terrorism Financing, Law of the Republic of Armenia on Protection of Personal Data, Central Bank of the Republic of Armenia (CBA) regulations, international documents, research articles, legal journals, and scholarly papers.

Certain legal instruments in terms of laws and other normative acts of the Republic of Armenia are also cited in the paper. The Central Bank Board Resolutions 188-N, 279-N, Regulation 8/03 and the Guidance on the Risk-Based Approach to combating Money Laundering and Terrorist Financing are also analyzed herein. The General Data Protection Regulation is one of the core documents to be discussed in this paper, which is a valuable contribution to present research by offering an insight into international best practices.

CHAPTER 1: Customer Data Protection in the Financial Sphere

Financial institutions possess a vast amount of information and data about their customers. They know how much money their customers have, also where and how often they spend it, hence they are uniquely positioned to understand their customer's businesses and craft targeted offers. Nevertheless, financial institutions have important reasons to collect and hold enormous information. For instance, if a bank or a credit organization is lending money it needs to know the borrower's income, assets and credit history. On the deposit side, customer personal data such as a social security number, mobile number or IP address helps authenticate the person accessing the account, thus guarding against fraud. Not least of all, financial institutions are required to gather and integrate more data to comply with regulations ranging from anti-money laundering and the "Know Your Customer" principle to Foreign Account Tax Compliance Act (FATCA) to conduct due diligence on applicants before opening accounts or lending money.

The identification and verification of the customer's component require a financial institution to collect information and identification from a customer upon entering into a contractual relationship. A question then arises: Is the customer well informed about how, when and how long this data will be used?

However, to provide evidence-based data a certain survey has been conducted throughout the Armenian bank customers. It turned out that 37.50 percent of respondents are not aware of how banks use and process their personal data, 56.25 percent are not aware of how long banks use and process their data, moreover, they are not aware of why this data is used and processed by banks.[14]

Online Lending Risks in Terms of Customer Data Protection

At the outset, it is important to note that along with the development of the IT sector, as well as to make people's lives easier, many banks and credit organizations use online banking systems to provide online loans and other services. The person can get a loan without going to the bank or at least he or she can fill out an online application for a loan, by providing certain personal data. According to the aforementioned survey results, 22.22 percent of the respondents used online lending.

It is important to point out the possible risks of data processing that can be adversely affected by online lending.

Currently, many Armenian banks and credit organizations use online lending practices. Some, of course, transfer the loan amount to their **current** customer's bank accounts, that is to say, that the loan disbursement method is **non-cash,** and some take advantage of online signatures. This, consecutively, implies that the customer does not physically obtain the loan, which is a risky process for the bank in terms of legislation, especially the RA "*Law on Combating Money Laundering and Terrorism Financing*", and for the client in terms of the RA *"Law on Protection of Personal Data"*.

In particular, when giving to a customer an online loan in this way, the possibility to conduct a proper customer due diligence when establishing a business relationship or concluding a transaction is almost impossible. The customer due diligence process involves identifying the customer (including the authorized person and the beneficial owner) and verifying their identity, identifying the purpose and intended nature of the business relationship, as well as ongoing due diligence throughout the business relationship (including the time of establishing a business relationship with the customer).

[14] Tatevik Kyandaryan, *Weather You are Aware how Your Personal Data are Used. (2020), available at* https://www.surveymonkey.com/r/VBDNC2P (last visited March 18, 2020).

Besides, the reporting entities shall undertake necessary measures to find out the existence of a beneficial owner and identify and verify his/ her identity, or where an authorized person acts on behalf of the customer, the reporting entity shall be obligated to identify such a person and verify his/her identity and his/her authority to represent the customer.[15] However, it is not possible to accomplish all this when lending online.

As already mentioned, banks and other financial organizations (e.g. credit organizations or microfinance organizations) typically check the borrower's personal data in detail and ask for a passport to compare a photo and signature. However, if you have lost your passport or it got stolen, the perpetrators can easily replace your photo, forge your signature and try to get an online loan on your behalf.

All financial institutions, of course, do serious due diligence about a potential borrower and his or her income before giving a loan. For this reason, the perpetrators prefer to deal with online loans provided by microfinance organizations. In this case, the verification is done with a simplified scheme. For example, microfinance organizations ask the borrower to send passport data or a document scan. In such cases, the perpetrators using modern technological tools (e.g. Photoshop), easily can change the passport holder's photo and falsify the signature. Perpetrators will be punished by the strictness of the law for these fraud actions, but if strict legislative approaches are in place it will be possible to prevent such actions, otherwise the procedure will be complicated and time-consuming for the customer.

It should be noted that when applying for any type of loan, financial institutions request to the ACRA Credit Bureau about the financial status of the potential borrower, which requires the applicant's written (including electronic) consent.[16] In such circumstances personal data is not fully protected, as in case of having any person's passport information, anyone can apply for an online loan and give the bank permission request to the ACRA Credit Bureau. In case the bank refuses to grant the loan, the already made request will harm the credit history of the respondent. It is also necessary to mention, that in case of refusal the bank retains the applicant's personal data, thus the applicant will not become the bank's customer as no actual transaction took place and business relations were absent.

[15] Republic of Armenia Law on Combating Money Laundering and Terrorism Financing, Art.16(5).

[16] Republic of Armenia Law On Circulation of Credit Information and Activity of Credit Bureaus No. HO-185-N, adopted on October 22, 2008, Art. 16(1).

It can be concluded that in this case, the bank cannot generally supervise the processing of its potential customer's personal data by the ACRA Credit Bureau, as the consent for processing the personal data is not executed by the real customer.

The Minimum Requirements for Banks and Credit Organizations to Process Their Customer's Data. "Know Your Customer" Principle

The principle of the "Know Your Customer" is a process to which financial institutions must adhere in order to comply with global Anti-Money Laundering regulations. It requires the institution to verify the identity of its clients and to obtain detailed due diligence information in order to assess the potential risk of illegal activity. Each financial institution must conduct appropriate due diligence to verify the identity of individuals, businesses and other entities with which it does business.[17] All financial institutions must have AML Policies, which recognize that KYC Procedures may vary by the jurisdiction or location of the financial institution.

Generally speaking, a financial institution's KYC process and an international company's Foreign Corrupt Practices Act due diligence process is as follows: first of all, customer identification documentation is collected along with other information provided by the customer, which is undoubtedly personal information. For instance, a bank or a credit organization can ask the customer to provide them information about the aim and reason of opening an account, source of funds, nature and scope of customer's activities, residence, etc. These are the minimum requirements by regulation.

Customer Due Diligence (CDD) is intended to authenticate the client's identity and trustworthiness of all cash flow sources involved in business relationships with clients. This consists of general identification requirements and specific identification requirements, including responsibility for updating all information about the client. Such inspection may also include obtaining information about the client's honesty and reputation.

CDD is intended to understand who the **Ultimate Beneficial Owner** (UBO) is. UBO is a natural person, who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or controls" and "ultimate

[17] 279-N CBA § 30 (2014 through October 27).

effective control" refer to the situations in which ownership or control is exercised through the chain of ownership or using control other than direct control.

Enhanced Due Diligence (EDD) is intended to ensure robust investigation, over and above required KYC Procedures, to verify a potential client's or contracting party's identity. In connection with procurement, this may include testing the customer or company's profile, including their background; examining possible links to illicit activities; identifying ultimate beneficial ownership of a company; investigating company executives, interviewing a company's vendors or other contacts to gauge the reliability of its previous business relationships; and researching whether a person or company has ties to government-owned entities.

Unfortunately, the law and regulation allow financial institutions to provide other risk assessment mechanisms, which allows them to ask the customer many other questions. While the due diligence and KYC processes vary, similarities exist when it comes to privacy concerns. These concerns include the collection, transfer and storage of customer documentation and collection and transfer of customer's personal information.

Applying the **"Know Your Customer"** principle allows financial institutions to form a sound belief that the institution possesses the necessary information about each customer, as well as an understanding of the types of transactions that the customer performs and/or is likely to perform.
The followings are core elements for financial institutions from the perspective of the KYC principle:

- Financial institutions are obliged to authenticate and verify each customer's identity,
- Financial institutions should take the necessary steps to identify the real beneficiary, and, if available, identify and verify his or her identity,
- If the customer is an authorized person, financial institutions are obliged also to identify that person, verify his or her identity and authority to act on behalf of the client,
- Financial institutions should obtain necessary information about the client's financial situation and trading activities, including the expected scope and nature of transactions.

In terms of legislation, of course, this is only done for the prevention of money laundering and terrorism financing.

Money laundering is the acquisition, possession or use and transfer of money, knowing that such money is derived from criminal activity or an act of participation in such activity, to conceal or disguise the illicit origin of the money or of assisting any person who is involved in the commission

of such activity to evade the legal consequences of his action as well as the concealment or disguise of the true nature, source, location, disposition, movement, rights concerning, or ownership of money or the participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of these actions.[18]

Money laundering is a serious threat to a country's economic system and has a negative impact on the integrity of financial institutions. It also changes the balance of economic power in certain sectors. If money laundering is not adequately controlled, it can cause societal corruption. "Money laundering generally involves a series of multiple transactions used to disguise the source of financial assets so that those assets may be used without compromising the criminals who are seeking to use them."[19] Every year, terrorists, drug lords, human traffickers, and other assorted criminals launder some $1.6 trillion in illicit funds across the globe. [20]

Anti-money laundering efforts fight against several factors. Money laundering can result in a reduction in public trust towards economic sectors such as financial institutions. Besides, investments in money received through criminal means may negatively affect the healthy competition between companies and entrepreneurs. Money laundering also allows criminals to continue and expand activities in formal sectors of the economy, potentially creating an impression that income can be earned and encouraging people to engage in criminal activity.

Effective controls help facilitate the identification of persons who commit offenses and prevent their illegal actions. Furthermore, providing information to the law enforcement agencies will initiate a criminal investigation and create a disincentive for future activity.

The Financial Action Task Force (FATF), which is an independent inter-governmental body, develops and promotes policies to protect the global financial system against money laundering and terrorist financing. [21] In 1990 FATF adopted "**the 40 Recommendations**" on combating money laundering which set standards that governments are expected to meet, with a special emphasis on the

---

[18] Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, Art. 1, (10 June 1991).
[19] US Department of State, *Economic Perspectives, The Fight Against Money Laundering*, available at https://web-archive-2017.ait.org.tw/infousa/zhtw/DOCS/ijee0501.pdf (last visited April 19, 2020).
[20] United Nations: Office on Drugs and Crime, *Illicit money: how much is out there?, available at* https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html (last visited March 18, 2020).
[21] FATF Guidance, *"Anti-money laundering and terrorist financing measures and Financial Inclusion", available at* https://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf (last visited May 3, 2020).

critical role that the financial sector has to play. It states that financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g., copies or records of official identification documents (e.g., passports, identity cards, licenses and similar documents), account files and business correspondence for at least five years after the business relationship is ended.[22] The measures would generally put more obligations to adopt ***Know Your Customer*** policies and enhance suspicious transaction reporting.

All financial institutions must have an effective risk-based Anti-Money Laundering/ Combating the Financing of Terrorism (AML/ CFT) system in place within their network. They must implement the highest standards and international best practices throughout their network in combating money laundering, terrorist financing and other acts punishable by law. Of course, the use of AML regulations is a necessary and mandatory requirement for financial institutions in Armenia as well, but one should not overlook the fact that customer data is not used solely to combat money laundering.

All over the world, as well as all banks and credit organizations in the Republic of Armenia have internal regulations, which guide the collection, use and procession of customer data, as well as conduction of proper customer due diligence.

The contractual relationship between financial institutions and a customer prohibits the financial institutions from disclosing information about the customer's data, affairs and accounts to third parties. However, there are exceptions to this confidentiality obligation. For instance, according to the law the processor may transfer personal data to third parties or grant access to data without the personal data subject's consent, where it is provided for by law and has an adequate level of protection.[23] Different state bodies (i.e. Central Bank of RA, courts, prosecutors and national security bodies, etc.) can require the personal data, **thus the financial organizations cannot provide the accurate list of these bodies to their clients which may require that information.**

Apart from this, Anti-Money Laundering regulations compel banks to report suspicious transactions without customers' knowledge and consent.

[22] *Id, at 39.*
[23] Republic of Armenia Law on Protection of Personal Data, Art. 26.

Types of Data Processing in Financial Institutions

Customer data can be divided into two categories: one, collected just to comply with the abovementioned regulations, and the other that can also be used to support sales and relationship management. Financial institutions understand the important data points when it comes to loans or deposits, most banks still could use help in collecting some of the basic information about their customers. Banks and credit organizations by the purpose and procedure established by law, Central Bank regulations and their internal policies acquire certain personal data and may use them for different purposes, such as customer profitability, direct marketing, AML ranking, etc.

1. Customer profitability

With business lines under ever more pressure to strengthen their competitive position through a better understanding of customers, adding just a few new questions to the customer onboarding process can help banks obtain potential new insights about client behavior. It is noteworthy that focusing too much on customer protection can limit innovation, preventing the development of products and services that create value for customers and businesses. Customer data are critical to innovation and growth, but data misuse risks a loss of trust that could destabilize the financial services system. The Internet drives innovation, productivity growth, and communication. But it is also a harbinger of data breaches, identity theft, and financial fraud, all of which have trended up during the Internet era. Users are rightly concerned about the protection of their personal information. Market confidence and consumer protection are undermined if the financial system is not adequately protected from abuses.

This data can also help banks identify their most profitable customers. Institutions have traditionally sought to boost profits through volume. On the obscurity side of the range, clients are each offering similar products and services. This empowers a high level of privacy with limited discrimination against protected classes; nonetheless, it might debilitate benefit, or even lead organizations to leave items or markets where the normal client is not beneficial.

More prominent accuracy takes into consideration more modified profiles for individual customers. This can profit customers with attractive risk profiles but it can also prevent high-risk

customers from gaining access to services. That is, it is necessary to balance the procession of customer data and all the risks arising therefrom.

2. Direct marketing

Personal data is often used by banks and credit organizations for marketing purposes. With the advent of new technology, product advertising through e-mail, automated calls, short message service (hereinafter SMS), multimedia messaging service (hereinafter MMS) and even with social media or another application has become an effective tool in commercial matters. These marketing activities begin with consumer research and end with satisfying consumer needs.[24]

Direct marketing is a common purpose of processing, and it includes several activities—e.g., collecting personal data from potential customers, creating profiles about those potential customers and their preferences, and then sending personalized communications to them.

With a myriad of options available to consumers for everything from standard banking services to investment management and sophisticated financial planning, every financial services provider must be mindful of the competition – and that means having a deep understanding of what attracts customers, what makes them loyal, and what keeps them happy. The main issues of direct marketing are to maintain a range of existing customers, to expand the list of services provided to regular customers and to attract new customers.[25]

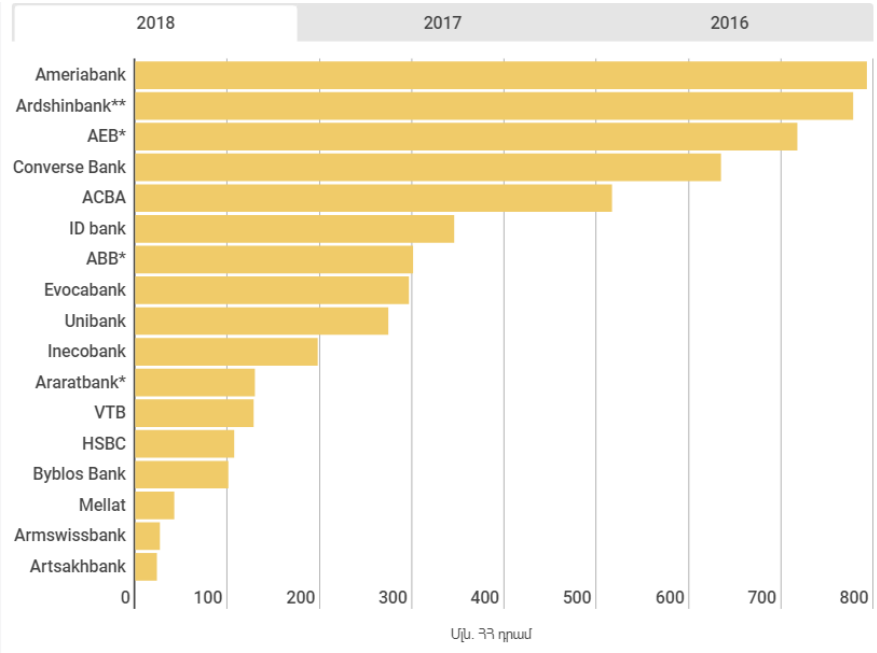
Consent and legitimate interests are the legal bases most likely to be relied upon to justify direct marketing. Where direct marketing involves electronic communications, however, is where things get complicated.

The banking system of the Republic of Armenia is not big; however, the competition is quite large. In order to attract depositors and reliable borrowers, banks compete not only with each other but also with credit and deposit organizations. It is important to point out, that advertising has its place in this competition. Armenian banks spend serious money on advertising and PR events.

The following picture shows the marketing costs (the numbers are presented in million AMD) of Armenian commercial banks for 2018. [26]

---

[24] Naira Hayrapetyan & Nune Hayrapetyan, *Bank Marketing, p. 23* (College of Finance and Banking, vol. 1) (2003).
[25] *Id, at 24.*
[26] Modex Advisory – Infogram, *Marketing Costs of Armenian Commercial Banks, available at* https://infogram.com/marketing-costs-of-armenian-commercial-banks-1h17497llyzq6zj (last visited March 15, 2020).



Overall, in 2018, commercial banks of the Republic of Armenia allocated billions for advertising and representation expenses. That is to say, the largest customer in the advertising market today is probably the banking system.

GDPR provides that individuals have the right to object to direct marketing.[27] When an individual exercises this right, the bank must not only stop sending direct marketing material to the individual but also stop any processing of that individual's personal data for marketing purposes. For example, in the case of an objection from a data subject, the bank should stop profiling that individual for the purposes of direct marketing.

Communication for direct marketing purposes of third party products or services other than the bank, which is conducting the advertising, that is, via conventional mail, electronic means or printed on any type of stationery issued by banks always requires the explicit consent of the customer.

GDPR requires that information about the right to oppose is appropriately given by the bank to its customers'.[28] In practice, this is normally done at the beginning of a relationship. If no objection has been/is being received, banks may continue to process these customers' data for direct marketing purposes by conventional mail.

[27] 2016/679 GDPR, § 21 (2) and (3).

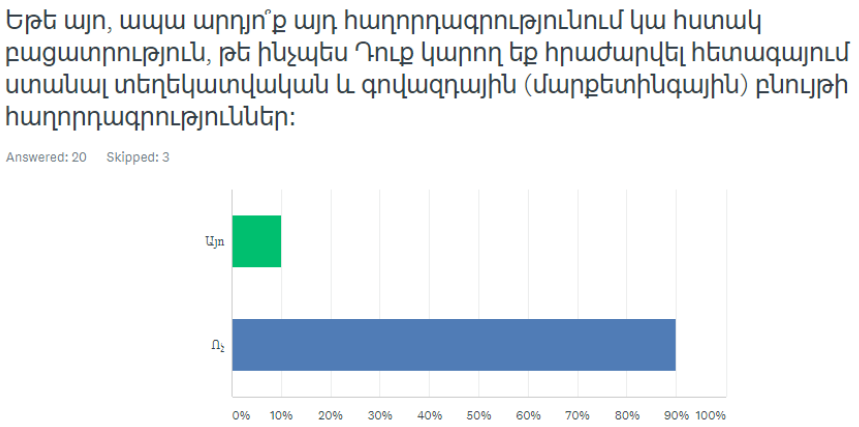
[28] § 13(2)(b).

In case of **withdrawal** of the data subject's consent given in writing, validated by signature, or electronically, validated by an electronic digital signature, the processor **shall be obliged to terminate the processing** of personal data and destruct the data within ten working days following the receipt of the withdrawal unless otherwise provided for by mutual consent of the data subject and the processor or by law.[29]

At the same time, it should be noted that Central Bank regulation states, that messages, which contain advertisements and that are sent to the customer's personal email address must meet a number of requirements, that is the message should provide a clear explanation of how the customer may refuse to receive informational and advertising messages in the future. Moreover, the explanation must be written distinctively (in other fonts, in different font sizes, in different colors or in other forms). [30]

The regulation clearly stipulates that any customer may exercise his or her right to refuse to receive emails containing promotional material, thereby limiting the procession of personal data by the financial organization. However, the results of a survey in the Armenian market have shown that many financial organizations, perhaps the majority, do not apply this law and bypass it.

The below picture shows the results of the survey, according to which 90 percent of customers do not receive any explanation for refusing to receive promotional materials.[31]



[29] Republic of Armenia Law on Protection of Personal Data, Art. 21(6).
[30] *8/03 CBA,* § 56(4) (2009 through September 30).
[31] Tatevik Kyandaryan, *Weather You are Aware how Your Personal Data are Used, available at* https://www.surveymonkey.com/r/VBDNC2P (last visited March 18, 2020).

Thus, the bank or the credit organization is obliged to provide a link to unsubscribe in case of sending advertisements to its customers. This regulation makes compulsory for companies to cease processing of data for commercial purposes. Preliminary agreement and opt-out right improves the situation of customers, on the one hand, it makes it difficult for the company's commercial services to operate, reducing the number of customers. On the other hand, opt-out is the process using which a user withdraws or refuses to give consent for certain actions to be carried out. This method provides the user with a fairly large amount of control over their data and other privacy settings. [32] Hence, the right granted to individuals comes to reinforce the idea of private life and to guarantee the privacy of everyone.

RA Law on Protection of Personal Data states, that the data being processed on the basis of consent shall be stored **for the period objectively necessary** for implementing the purposes of processing data or for the period prescribed by the consent, whereas banks and other financial organizations collect, store and process the personal data of their current and former customers, for the purpose of KYC principal and use that data for marketing purposes, and do not stop processing them even when the grounds and purpose of the processing of data are eliminated.

In practice, when banks ask a question to a customer, they do not inform that the question comes from the "Know Your Customer" principle required by law, and these other questions are for marketing purposes. By the way, income, loans to other banks, and other information about a customer and his/her family members are often collected. Unfortunately, all this may be presented as an application of the "Know Your Customer" principle. The CBA Regulation and the Law on Combating Money Laundering and Terrorism Financing have left such a discretion without defining a specific framework for the processing of personal data. Thus, when collecting data in such an inappropriate manner, the financial organization may lose its client because the latter may think that financial organization violates his/her right to privacy.

[32] Cookie Law Info, *What is Opt-in and Opt-out in GDPR?, available at* https://www.cookielawinfo.com/what-is-opt-in-and-opt-out-in-gdpr/ (last visited March 22, 2020).

CHAPTER 2: Data Protection Mechanisms in Europe

The regulation of privacy started with the publication of the guidelines surrounding data privacy from the organization for **Economic Co-operation and Development (OECD)**. On 23 September 1980, they published eight principles for the processing of personal data.
These eight principles were:

1. **"Collection limitation** - there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[33]
2. **"Data quality** - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[34]
3. **"Purpose specification** - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[35]
4. **"Use limitation** - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a) with the consent of the data subject, or
   b) by the authority of law."[36]

[33] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Art. 7 (September 23, 1980).
[34] *Id*, § 8.
[35] *Id*, § 9.
[36] *Id*, § 10.

5. **"Security safeguards** - personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."[37]
6. **"Openness** - There should be a general policy of openness about developments, practices and policies concerning personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[38]
7. **"Individual participation** - An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."[39]

8. **"Accountability principle** - A data controller should be accountable for complying with measures which give effect to the principles stated above."[40]

These principles were conceived to protect the personal data of consumers. Even if this set of principles is 40 years old, it is still relevant today. Many European countries made their national privacy regulation based on the OECD guideline.

The EU implemented the **"Data Protection Directive 95/46/EC"** on 24 October 1995, which was based on the guidelines of the OECD. It was conceived to harmonize the data protection laws of the EU member states. Despite the attempt of the EU to harmonize the privacy regulation, directive 95/46/EC was not sufficient, EU parliament has come up with the initial proposal for an updated data protection regulation – **GDPR**, which has been approved on 14 April 2016 and came into force on 25 May 2018. This law is designed to harmonize data privacy laws across Europe and protect the

[37] *Id*, § 11.
[38] *Id*, § 12.
[39] *Id*, § 13.
[40] *Id*, § 14.

personal data of all EU. GDPR aims at giving data subjects in Europe greater control over their personal data and ensure the free movement of these data in the European internal market.

There are some key changes, that GDPR brought:

1. The territorial scope is increased. Every company that trades with the EU has to obey GDPR. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union.[41]
2. The penalties have been increased drastically: up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[42] The fines must be effective, proportionate and dissuasive for each individual case. For the decision of whether and what level of penalty can be assessed, the authorities have a statutory catalogue of criteria which they must consider for their decision.[43]
3. Consumers have to give explicit consent for the data processing through an easy and accessible form.[44] Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing.[45]
4. The consumer has the right to be forgotten.[46] The right to be forgotten derives from the case *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014).*[47] For the first time, the right to be forgotten is codified and to be found in the General Data Protection Regulation in addition to the right to erasure[48]. Before GDPR, in Europe, the intellectual roots of the right to be forgotten could be found in French law, which recognized ***le droit à l'oubli*** or the ***"right of oblivion"*** **-** a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the

[41] 2016/679 GDPR § 3.
[42] § 83(5).
[43] 2016/679 GDPR Fines / Penalties.
[44] § 7.
[45] 2016/679 GDPR Consent.
[46] § 17(2).
[47] *Google Spain, Google Inc v Agencia Espanola de Proteccion de Dataos (AEPD), Mario Costeja Gonzalez* (2014), ECJ C-131/12.
[48] 2016/679 GDPR Right to be forgotten. https://gdpr-info.eu/issues/right-to-be-forgotten/ .

facts of his conviction and incarceration.[49] Under GDPR, a company has to erase the data of consumers on request. Individuals can request erasure verbally or in writing. Company has one month to respond to a request. The right is not absolute and only applies in certain circumstances. This right is not the only way in which GDPR places an obligation on the data processors to consider whether to delete personal data or keep processing it.

5. Public authorities and large organizations that process data on large scale have to appoint a Data Protection Officer (DPO).[50] GDPR makes the appointment of DPOs **mandatory** in any case where the entity:
    a. is a **public authority** or body (except for courts acting in their judicial capacity)
    b. pursues core processing activities which require **regular and systematic monitoring** of data subjects on a **large scale**,
    c. pursues core activities which consist of processing of **sensitive data** on a **large scale**.
    [51]

Where appointed, the DPO must be involved "*properly and in a timely manner, in all issues which relate to the protection of personal data*"[52] and, in particular, must be tasked with informing and advising the entity and its employees of their data protection obligations,[53] monitoring compliance,[54] and liaising and cooperating with the DPA.[55] The contact details of the DPO including through general publication[56] and data subjects may contact them any data protection issue.[57]

GDPR at Banks and Financial Institutions

Financial institutions process a vast amount of personal data on a daily basis. Much of the data processed is confidential and sensitive. GDPR aims to protect personal data, making it easier for consumers to know where their data is being used and raise objections about its use. GDPR has had a

[49] Jeffrey Rosen, *The Right to be Forgotten,* 64 Stanf. L. Rev. Online 88 (2012).
[50] 2016/679 GDPR§ 38.
[51] §37(1)
[52] §38(1).
[53] §39(1)(a).
[54] §39(1)(b).
[55] §39(1)(d)-(e).
[56] §37(7).
[57] §38(4).

strong impact on financial institutions as they process a large amount of personal data. Every process of GDPR implementation in financial institutions should start with an analysis of their resources.

To ensure that customer personal data is always under control and that the process of GDPR implementation in banks is efficient, a Personal Data Controller should be appointed.

Each bank and credit organization that processes personal data need a legitimate basis for processing. GDPR provides that processing shall be lawful only if and to the extent that:

- ✔ the data subject has given consent,
- ✔ the processing is necessary for the performance of a contract with the data subject,
- ✔ it is necessary for the compliance with a legal obligation or a task carried out in the public interest,
- ✔ it is necessary to protect the vital interests of an individual, or
- ✔ it is necessary for the purposes of legitimate interests of the controller or another third party, as long as they do not contradict the fundamental rights of the data subject.[58]

Often, financial organizations process personal data in order to fulfill their duties (for instance an account agreement, loan contract, KYC procedures, etc.) because they have a legal obligation to do so. GDPR does not restrict the KYC operations of an organization, rather recognizes the importance of identity and ensures its protection. GDPR, at its core, merely emphasizes better protection of data subjects by directing how information is collected, processed and used. GDPR imposes strict limits on the processing and sharing of personal information, posing a real barrier to efficient AML and KYC procedures alike. It is important to mention, that the request for consent shall be presented in a manner that is distinguishable from the other matters.[59] It can be concluded that the customer gave his/her consent to the bank or credit organization for processing of such data for a specific purpose.

Nevertheless, some banks use ***explicit consent*** *under GDPR,* and take the path of sending privacy notes to customers which are very detailed, explicitly mentioning the **KYC** identification and verification processes as well as the background screening for Politically Exposed Persons and sanctions. Hence, banks need to perform due diligence more selectively, meaning that data being processed must add value to the KYC process. After KYC onboarding, customers have more control

[58] § 6.
[59] §7(2).

over their information. The process of obtaining, storing, and managing data must be transparent to customers. As an example, in October 2017 United Kingdom **Information Commissioner's Office reviewed 30 websites** in the retail, banking and lending, and travel and finance price comparison sectors and found, that:

- 87% failed to adequately explain whether they share data with third parties and, if so, who.
- 87% failed to specify how and where information would be stored (important especially in the event of international transfer).
- 23% did not make it clear how a user could access the data held about them.
- 80% did not refer to their retention policy.[60]

Thus, financial organizations in contact with such information, will need to ensure the security of information in a manner that conforms to GDPR guidelines. Additionally, they need to make the use of information very clear, easy to understand and transparent for individuals. Meanwhile, GDPR does not apply to data of legal entities.[61] Thus, the application of GDPR had only a minimal impact on the processing of data relating directly to legal entities. Such data typically include the name (business name) of the corporation, the legal form, the address of its registered office or the individual sites, as well as (working) contact details of natural persons (telephone, e-mail address, etc.) acting on behalf of the corporation. It turns out that the data of legal entities, which are also customers of the financial organizations, are generally not protected under GDPR, thus there is a legislative gap.

Direct Marketing Under GDPR

Banks use different ways to reach out to clients. One of the main ways is the use of direct marketing, which, however, is not specifically defined in GDPR. GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.[62]

---

[60] International Commissioner's Office, *International enforcement operation finds website privacy notices are too vague and generally inadequate*, *available at* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/international-enforcement-operation-finds-website-privacy-notices-are-too-vague-and-generally-inadequate (last visited March 25, 2020).

[61] 2016/679 GDPR Recital 14.

[62] Recital 47.

Hence, legitimate interests can be used to satisfy GDPR's legal basis requirement. Marketing emails may be sent on an opt-out basis if the recipient's details were collected *"in the context of the sale of a product or a service".*[63] Legitimate interests of the bank include, for example, a situation where there is a specific relationship between the controller of personal data and the data subject (typically the client's relationship with the bank).

It is important to note, that GDPR states that where personal data are processed for direct marketing purposes, the data subject shall have the right to **object** at any time to processing of personal data concerning him or her for such marketing and that where the data subject objects to processing for direct marketing purposes, the personal **data shall no longer be processed** for such purposes.[64] As a further matter, this right must be *explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information*.[65] This indicates, that even if opt-in consent is not required before sending marketing emails, GDPR nevertheless requires that the recipient always be provided with an opportunity to opt-out of receiving such emails. Hence, there is a need to include **a specific** opt-out in every marketing message to allow individuals to withdraw their consent at any time.

CHAPTER 3: Recommendations Aimed at Legal Regulation Changes

The information presented in the previous two chapters allows discussing the parallels between Armenian and international legislation and presenting recommendations grounded on the analysis of the issues discussed therein.

First of all, it is important to highlight, that RA Law on Protection of Personal Data is largely consistent with GDPR, however, certain changes will contribute data subjects to be more secure. Furthermore, one of the focal points of GDPR concerns the appointment of a Data Protection Officer. GDPR stipulates in which cases the designation of a data protection officer is mandatory and what their typical responsibilities are. DPO shall monitor compliance, inform and advise data controllers, data processors and all employees who carry out personal data processing, cooperate

[63] *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector,* The European Parliament and The Council, Article 13(2), (July 12, 2002).
[64] 2016/679 GDPR§ 21 (3).
[65] *Id,* § 21(5).

with supervisory authorities and act as the single point of contact for data subjects regarding their rights.

Under the RA Law on Personal Data Protection an impartial and permanent monitoring body for the processing of personal data has been established - the **Personal Data Protection Agency**. It was established as a separate unit of the Ministry of Justice of the Republic of Armenia.The Agency shall carry out functions provided for by the Law of the Republic of Armenia "On protection of personal data" to implement its goals and objectives.[66] The Agency is authorized to apply administrative sanctions in cases of violations of the Law on Personal Data Protection, and in cases stipulated by law to apply to court. The decisions of the agency can be appealed in court.

The **Personal Data Protection Agency** operates independently.[67] At the same time, the law states, that the head of the agency is appointed by the Prime Minister of the Republic of Armenia for a term of five years upon the recommendation of the Minister of Justice of the Republic of Armenia. [68] Thus, in case of any violation of the law on Personal Data Protection, the agency is the body that solves all kinds of issues and makes decisions.

RA Law on Protection of Personal Data does not oblige large organizations to have a DPO, while it would be a great idea **to oblige banks and financial organizations to appoint a DPO**. By developing a data protection culture, the DPO, through his action, will enable the organization to strengthen the relationship of trust with its customers and partners.

Second, the Central Bank of Armenia should remove all discretionary provisions from the Regulation on Minimum Requirements for Reporting issuers for the Prevention of Money Laundering and Terrorist Financing provided to the banks and credit organizations. The "Know Your Customer" principle should be neither minimal nor infinitely permissible - it should be clear. The due diligence of the customers must also be targeted in order to maintain the provisions of AML regulations. Of course, banks are entitled to ask additional questions to the customers for commercial purposes, but this **should not be done** as a matter of applying the ***"Know Your Customer"*** principle.

Third, banks do not have a list of questions which they ask while opening an account and an explanation of the "Know Your Customer" principle on their websites. CBA Regulation 8/03 states, that each financial institution should have an information, that ***"In order to perform customer due***

[66] *Charter of the Agency for Protection of Personal Data of the Ministry of Justice of the Republic of Armenia,* Art. 8.
[67] Republic of Armenia Law on Protection of Personal Data, Art. 24 (2).
[68] § 25 (1).

diligence, as required under the Republic of Armenia Law on Combatting Money Laundering and Terrorism Financing, the Bank may request you to provide additional documents or other information as part of its "Know your customer" procedures or ask additional questions during verbal communication (if required). [69] ***According to the agreement signed with the US under the Foreign Account Tax Compliance Act (FATCA)) the Bank may collect additional information to find out whether you are a US taxpayer."*** [70]

We can definitely state, that this is quite an adequate step, but at the same time the customer does not understand what the "Know Your Customer" principle is.

Any person is reluctant to give personal information to a "stranger". At least he or she should be told why there is a need to report such information. Employees of the bank should also be trained in this field and explain the meaning of the questions and the reasons of asking such questions when communicating with the client. In general, the term "Know Your Customer" is self-explanatory. This term should become part of financial literacy; all clients should know it.

The effectiveness of bureaucratic mechanisms to combat anti-money laundering and terrorism financing is not so clear. It seems that the harder the bureaucracy gets, the more effective the criminals find ways to circumvent it. In fact, an honest person gets annoyed when he/she is asked to provide personal information. Whereas, criminals deal with these issues in an act of preparation and with appropriate papers.

Fourth, in addition to the minimum requirements for banks, the Central Bank should also set "maximum" requirements for banks to process customer's data. Often, and it can also be said unintentionally, the bank begins to possess and process more personal data than required by law. In the Republic of Armenia, there is a serious problem of leakage of personal data through the banking system. Let's put aside the fact that some banks, when approving their internal policies, set their wishes above the laws in the Republic of Armenia. For instance, the Tax Code of the Republic of Armenia does not oblige an individual entrepreneur to have a separate account, but banks force to open a separate account.

[69] 8/03 CBA Chapter 4, § 17(9) (k).

[70] § 17(9) (l).

Banks, when opening accounts for organizations, often require not only the state certificate and company charter but also the minutes of the founding members, where the personal data of the participants are clearly stated.

The question arises as to why the bank requires such a document if the transactions are performed by two persons: **the president and the accountant**. It can be assumed that the bank attracts additional customers and collects its data.

In many cases people provide the data of founding members of their organization, however the latter has nothing to do with the current bank and, likely, would not want a third party to possess his/her personal information. Personal data obtained as a result of such requests can in no way be considered as personal data obtained as a result of due diligence of the customer and for the KYC principle, as in this case, the financial institution starts to process the personal data of third/physical persons.

Fifth, an appropriate change must be made in RA Law On Circulation of Credit Information and Activity of Credit Bureaus. It is worth to mention that credit reports, information and other services containing data, which identify the subject of credit information may be received only by the written consent (including by electronic letter) of the subject of credit information.[71] This will certainly complicate the process of online lending, but until there is no other way to identify the customer and the real beneficiary, the inquiries should only be made on the basis of **written**, but non-electronic agreements. At the same time, it is necessary to clearly limit the possibility of applying for online lending by the ones who are not customers of that financial organization yet.

Moreover, there is also a contradiction from the point of view of the law of personal data, since by law the data subject shall give his or her oral consent by means of such reliable operations which will obviously attest the consent of the data subject on using the personal data.[72] Thus, it is necessary to exclude the possibility of oral consent.

Financial organizations shall ensure that all their loan contracts include a short, but clear explanation of how client data will be protected, how it may be used or shared and with whom. In particular, the following can be used as an example: "***The Lender shall ensure the protection of personal data collected and used within the scope of this Agreement per the requirements of the legislation of the Republic of Armenia, shall undertake such technical measures and shall***

[71] Republic of Armenia Law On Circulation of Credit Information and Activity of Credit Bureaus, Art. 16.
[72] Republic of Armenia Law on Protection of Personal Data, Art. 9(7).

establish such organizational rules which are necessary for the proper maintenance of the Borrower's personal data. The Lender shall undertake reasonable steps to prevent the illegal disclosure of the Borrower's personal data stipulated by the legislation of the Republic of Armenia, which has become known in the scope of performed work (service provision) by its employees, as well as individuals and/or companies."

CBA Regulation clearly states that the messages that contain advertisements and that are sent to the customer's personal email address shall provide a clear explanation of how the customer may refuse to receive such messages in the future however, it only provides the possibility for **opt-out.** [73]

According to the international direct marketing experience there are two mechanisms for direct marketing: opt-in and opt-out. In the case of an opt-in mechanism, the data subject gives his or her prior consent to the processing of personal data. In this case, the customer, while receiving the advertisement containing messages, will have a possibility to reject the subsequent receipt of such messages. In the case of opt-out, the data subject refuses further processing of his/her data.

It would be much better if the CBA would also oblige banks and credit organizations to use **the opt-in mechanism,** that is, the customer will subscribe and will give his/her consent to receive messages which contain advertisements.

Finally, it is necessary to balance the period of data usage in terms of the money laundering legislation. As already mentioned in this paper, article 22 of the RA Law on Combating Money Laundering and Terrorism Financing stipulates that "[r]eporting entities **should maintain** the information (including documents) required under this Law, including the information (documents) obtained through customer due diligence, **regardless of the fact whether the transaction or business relationship is an ongoing one or has been terminated…"**

It is obvious, that the RA Law on Combating Money Laundering and Terrorism Financing does not set a precise period for the processing of personal data of customers of reporting entities (e.g. banks, credit organizations), which in its turn is a violation of RA Law on Protection of Personal Data. According to the RA Law on Protection of Personal Data the data being processed on the basis of consent shall be stored for the period objectively necessary for implementing the purposes of processing data or for the period prescribed by the data subject's consent.[74] It is necessary to make

[73] 8/03 CBA § 56(4).
[74] Republic of Armenia Law on Protection of Personal Data, Art. 9(2).

the appropriate adjustment and set a **clear timeframe**, after which the customer's data collected and processed based on the "Know Your Customer" principle will also be destroyed.

Conclusion

Given what has been outlined in the present paper in terms of the data protection regulation, it should, however, be highlighted that there are still major gaps in the legislation of the Republic of Armenia. The different comparative analysis had been drawn in this study aiming to answer the

question whether the use of a client's personal data for the reasons other than the intended purpose by financial institutions is lawful under Armenian law where the data was collected for conducting client due diligence based on the “Know Your Customer" principle”.

In the first chapter of this paper the current issues of data protection in financial sphere are discussed. The types of data processing, in particular customer profitability and direct marketing are analyzed. It studied current problems and presented statistics and relevant survey analysis. The first chapter also specified the minimum requirements for Armenian banks and credit organizations through which they are obliged to protect their customer data, including proper customer due diligence and highlighted the risks of online landing in terms of customer data protection.

In the frameworks of second chapter, the data protection mechanisms in Europe are analyzed. In particular OECD guidelines and GDPR are presented. It concluded, that AML and anti-corruption regulations, which require a company to conduct due diligence on those entities and individuals they intend to do business with, can conflict with international data privacy regulations. At the same time, proper due diligence and knowing the customer can lead to the prevention of corruption, money laundering and even terrorism. Failing to uncover the unlawful activity can lead to criminal or civil liability, fines and reputational damage. Failing to treat data privacy compliance with the same duty of care as other compliance obligations can lead to the same consequences. Thus, the conflict between data privacy provisions and regulatory compliance requirements is set to take center stage over the future. Financial institutions need a way to navigate through this complexity to find a way forward that ensures compliance but does not sacrifice operational efficiencies or client experience.

As for the third chapter, the parallels between Armenian legislation and international law are discussed with a view to revealing gaps of Armenian legislation hindering proper implementation of customer data protection.

Based on conducted research, the following recommendations are provided:

1. Customers should have a right to opt-in and opt-out at any time for receiving advertisements via e-mails or via SMS/MMS.
2. Each financial organization should be obliged to clearly explain to its customer why it collects detailed information, moreover, the client should know what specific questions are mandatory for implementing the KYC principle.

3. Banks and credit organizations should appoint a DPO, who will manage and find legitimate aim to keep and process the customer data. The Data Protection Officer in a bank or other financial institution sits clearly in the risk management and compliance oversight functions.

4. The Central Bank should set "maximum requirements" for banks to process customer's data, in order to satisfy **AML** requirements and limit access to customer data only to those users entrusted to collect and process such data as part of **KYC** activities and transaction monitoring alerts.

5. Financial organizations must have in place a general privacy policy covering all types of data processing. They should also have internal privacy policies dealing with the processing of specific types of personal data, where they should clearly state that the information collected for the KYC principle will not be used for commercial purposes.

This paper sought to paint a picture of the size of the challenge facing financial institutions with respect to emerging data privacy concerns and legislation and the impacts these inevitably will have on financial institutions challenged with implementing a raft of financial regulatory obligations.

The paper has elaborated and raised issues in terms of what financial institutions need to do to begin to comply with both data privacy and regulatory compliance obligations.

However, the key for banks to take full advantage of vast amounts of customer data lies in developing their ability to share it and the insights gleaned from it. As banks are redesigning their customer data systems and processes, they should do so creatively, with plans for using this data to serve multiple masters. Financial organizations are expected to gather and integrate more data on clients to comply with regulations ranging from anti-money laundering and KYC to FATCA.

List of Sources

Regulations

1. 8/03 CBA, available at https://www.arlis.am/DocumentView.aspx?docid=133371 .
2. 279-N CBA, available at

   https://www.cba.am/Storage/EN/FDK/Regulation/Regulation_Minimum_Requirements_eng.pdf .
3. Republic of Armenia Law On Circulation of Credit Information and Activity of Credit Bureaus No. HO-185-N, adopted on October 22, 2008, available at https://www.arlis.am/DocumentView.aspx?docid=120650 .
4. CBA Guidance for Financial Institutions on AML/CFT Risk Based Approach, available at https://www.cba.am/Storage/AM/downloads/FDK/Regulation_old/guidence_for_financial_institutions_on_amlcft_risk_based_approach_arm.pdf .
5. Republic of Armenia Law on Protection of Personal Data No. HO-49-N, adopted on May 18 2015, available at http://www.foi.am/u_files/file/Personaldataprotectionlaw_ENG.pdf .
6. Republic of Armenia Law on Combating Money Laundering and Terrorism Financing, No. HO-80-N, adopted on May 26, 2008, available at https://www.cba.am/Storage/EN/FDK/Regulation_old/law_on_combating_money_laundering_and_terrorism_financing_eng.pdf .
7. Council of Europe European Convention on Human Rights, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf .
8. Charter of the Agency for Protection of Personal Data of the Ministry of Justice of the Republic of Armenia.
9. *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector,* The European Parliament and The Council, Article 13(2), (July 12, 2002) available at https://eur-lex.europa.eu/eli/dir/2002/58/oj .
10. Guide on Article 8 of the European Convention on Human Rights, available at https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

1. Council of Europe General Data Protection Regulation, adopted on 14 April 2016, available at https://gdpr-info.eu/ .
2. Charter of Fundamental Rights of the European Union, adopted on 2 October 2000, available at https://www.europarl.europa.eu/charter/pdf/text_en.pdf .
3. Council of Europe e-Commerce Directive 2000/31/EC, adopted on 8 June 2000, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000L0031 .
4. Council of Europe Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973), available at https://rm.coe.int/1680502830 .
5. Council of Europe Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (1974), available at https://rm.coe.int/16804d1c51.
6. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (January 28, 1981), available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
7. Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, (10 June 1991).
8. Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on free movement of such data (1995), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML .

Books and articles

9. Frits W. Hondius, *A Decade of International Data Protection*, 30 Netherlands Intl. L. Rev. (1983).
10. Naira Hayrapetyan & Nune Hayrapetyan, *Bank Marketing,* (College of Finance and Banking, vol. 1) (2003).
11. Warren Samuel & Louis Brandeis, *The Right to Privacy*, (Harvard Law Review, vol. 4 (5)) (1890), available at http://www.jstor.org/stable/1321160 .
12. Tzanou Maria, *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures,* (Journal of Internet Law, vol. 17) (2013).

13. Tzanou Maria, *The Fundamental Right to Data Protection, Normative Value in the Context of Counter-Terrorism Surveillance* (2017).
14. Wesselin, Mara, *The European Fight against Terrorism Financing, Professional Fields and New Governing Practices* (Boxpress) (2013).
15. World Economic Forum, *The Appropriate Use of Customer Data in Financial Services, available at* https://www.weforum.org/whitepapers/the-appropriate-use-of-customer-data-in-financial-services .
16. Barry Barber, *Data Protection: Everybody's Business*, (1998).
17. Roger Cornwell & Marie Staunton, *Data Protection: Putting The Record Straight: The NCCL Guide to The Data Protection Act*, (1985).
18. Jeffrey Rosen, *The Right to be Forgotten,* 64 Stanf. L. Rev. Online 88 (2012), available at http://heinonline.org/HOL/Page?handle=hein.journals/slro64&div=17&g_sent=1&casa_token=&collection=journals .
19. Bygrave Lee, *Data Privacy Law: An International Perspective,* Oxford University Press (2013).
20. Van Alsenoy Brendan, *Allocating responsibility among controllers, processors, and 'everything in between': the definition of actors and roles in Directive 95/46/EC,* (Computer law and security review, vol. 28) (2012).
21. Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think,* (2013).
22. Rauhofer Judith, *Of Mice and Men: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?,* (European Data Protection Law, vol. 1(1)) (2015).
23. Cavoukian Ann, *Privacy by Design: Leadership, Methods and Results* (2013).
24. Kuner Christopher, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, (OECD Digital Economy Papers, No. 187, OECD Publishing) (2011) available at http://dx.doi.org/10.1787/5kg0s2fk315f-en .