Research and Science Today
WWW.RSTJOURNAL.COM

DOI: 10.38173/RST.2023.25.1.5:61-69

Title:	*PERSONAL DATA USE AND CONSUMER AWARENESS IN THE FINANCIAL SECTOR*
Author:	Laura Elly NAGHI

Section: Economics

Issue: 1(25)/2023

Received: 4 January 2023	**Revised:** 22 February 2023
Accepted: 9 March 2023	**Available Online:** 15 March 2023

Paper available online HERE

RST Research and Science Today
WWW.RSTJOURNAL.COM
SPRING 2023
No. 1(25)/2023
ISSN-P: 2247-4455 / ISSN-E: 2285-9632

Economics

PERSONAL DATA USE AND CONSUMER AWARENESS IN THE FINANCIAL SECTOR

Laura Elly NAGHI[1]

ABSTRACT:
THE LATEST TRENDS IN USE OF PERSONAL DATA BY THE ENTITIES OF FINANCIAL SECTOR MAY BRING ADVANTAGES FOR THE END-USER AS A TAILOR-MADE OFFER OF FINANCIAL SERVICES MAY BE MORE APPROPRIATE AND CHEAPER. BUT THIS OPPORTUNITY INCLUDES ALSO SOME RISKS AS THE AMOUNT OF DATA CENTRALIZED BY THE FINANCIAL INSTITUTIONS OR THE EXTEND TO WHICH THOSE DATA ARE USED MAY BE RESPONSIBLE FOR NEGATIVE RESULTS (CYBER-CRIME OR REJECTION OF CUSTOMERS). THE ARTICLE IS INTENDED TO EMPIRICALLY EVALUATE WHETHER THERE IS A LINK BETWEEN THE IMPROVEMENT IN THE GDPR USE AND THE FINANCIAL LITERACY OF THE FINAL CONSUMER OF FINANCIAL SERVICES. BASED ON A QUALITATIVE ANALYSIS OF THE REGULATION IMPLEMENTED AT INTERNATIONAL LEVEL, THE PAPER SUMMARIZES THE MAIN CONCERNS OF THE NATIONAL AUTHORITIES IN ORDER TO IMPROVE THE PROTECTION OF THE CUSTOMER BY RAISING AWARENESS OF THE USE OF HIS/HER PERSONAL DATA BY THE FINANCIAL SERVICE PROVIDERS.THE ANALISYS MAY BE USEFUL FOR THE PERSONAL DATA OPERATORS AS THEY MAY ADAPT THEIR INTERNAL POLICY TO BE COMPLIANT WITH THE LATEST PROVISIONS.

KEY WORDS: PERSONAL DATA, CONSUMER, FINANCIAL LITERACY, DATA BREACH

INTRODUCTION

The development of international financial services based on technological advances, globalization and the recent pandemic episode brought about a significant increase in the range of financial services offers for the final user. Due to the necessity to adapt the financial services as best as possible to the situation of each customer/ potential client, the financial sector has strived to collect, analyze and store an increasing volume of personal data. As the client was unaware of the ways in which his/her data were centralized, stored or transferred among the financial institutions having access to their data, the implementation of General Data Protection Regulation (GDPR) in 2018 was considered to be overly due as fraud schemes of personal data were registered in all economies. Similar concerns have been noticed also in the other sectors of activity such as health and telecommunications as the analysis of GDPR impact on the financial performance of the personal data operators was carried out empirically [1]. The adaptation of the internal procedures brought about

[1] Associate Professor PhD, Bucharest University of Economic Studies, Department of Finance, Romania, laura.naghi@fin.ase.ro.

significant changes and generated financial expenses that impacted their ordinary business as the entities focused on overcoming the barriers identified such as extensions, subjectivity, lack of budget or required technology [2]. On the other hand, a successful GDPR implementation was possible due to risks identifications and process documentation – the providers dealing with significant volume of personal data were required to manage the data and in this regard were careful about raising awareness about GDPR and applied minimum security measures.

Due to GDPR, online consumers were required to consent to the use of their personal data and by opt-in behavior, the providers of services had gained more efficiency in marketing projects and contractual lock-ins due to active elicitation of data use [3]. Despite expectations, GDPR implementation had zero effects on the indicators of international networks exchanges – there were limited influences on the number of observed agreements or on the number of customers of the network in the analysis of internet interconnections [4]. One intriguing issue concerning GDPR refers to de-identification of the personal data by the processors of data – the pseudonymization being one of the solutions in this regard – unfortunately the entities dealing with personal data do not see the benefits of using this process as GDPR is not offering sufficient incentives for them (such as limitation of liability) [5]. When combining the requirements of the GDPR with the developing technologies of Internet communications and online services, the question of data controlling by processing operators (such as Google Assistant or third-party programs) brings about concerns for correctly identifying the joint controllers [6].

The strict restrictions applied to financial institutions came as an important burden in the first years of implementation as new compliance procedures had to be developed and applied by the entities active in the financial sector – be it banks, insurance companies or investment funds a.s.o. On the other hand, the lack of understanding financial issues may position the client in the fragile situation of offering too much personal data information or missing the verification of the financial institution and therefore, may be opened to cybercrime attempts. Financial literacy projects promoted by national financial regulators or professional associations in the financial markets have undertaken the task of raising awareness of the adults to pay attention to the specifics of the financial services or activities of the financial institutions so that misleading attempts of accessing personal data to be diminished.

ANXIETIES GENERATED BY GDPR IN FINANCIAL SECTOR

The General Data Protection Regulation implied compliance of the service providers, no matter the industry, with clauses concerning collecting, analyzing and storing personal data. The European Regulation defines personal data as “any information that relates to an identified or identifiable living individual” and stresses upon the obligation of de-identification of the data in order to carry out analyses or forecasts. Before the implementation of the regulation, a third of the companies questioned by Deloitte in a benchmark survey estimated a cost of 100000 euro to be GDPR compliant as less than 20% estimated more than 5 million euros [7]. Even before the regulation 45% of the companies were offering dedicated privacy functions. The ambiguity of the requirements and the potential for significant fines determined the financial sector institutions to hast in their efforts to adapt their policies and procedures for the moment of GDPR application in May 2018.

After 5 years from the implementation of GDPR in Europe, there are still concerns in the financial services sector as the institutions are still struggling with some hotspots in this

area, such as the international transfer of personal data (mainly referring to European Union – US transfers), data breach response or even Brexit implications. The issues raised by the insufficiency of the Privacy Shield in transfers of data to the United States generated the obligation of taking detailed transfer impact assessments in terms of legislations and practices of the countries destined to receive the personal data. Moreover, the European Union developed new versions of the standard contractual clauses which must be applied by all the financial services firms that are to comply with transfer of data outside EU.

The pandemic of 2020 generated the necessity for the financial firms to adapt their activity by employing online tools – this adaptation became a competitive advantage for all those that were quick to offer new types of client relationship mechanisms (online sales, online servicing). Unfortunately, the speed of implementing the new approach gave way to cyber-exposures for themselves and for their clients and cases of data breach were reported all over the world in the financial sector. Stress testing of such procedures became the top priority of the financial firms as prevention was insufficient and appropriate data breach management could significantly diminish the probable losses. The concern of the financial firms in the last 3 years is obvious in the decision of assessing the degree of data breach in order to justify the notification (the companies have to decide in advance the volume and the type of data that would create the necessity to notify); the reporting obligations (according to the data protection legislation and also to the cyber-risk insurance contract, if existing) and the identification of key persons to be active in case of data breach response.

Besides the necessity of each national market to implement a comprehensive financial consumer protection framework that will provide safety even for online activities, the existence of national authorities that will take act in case of personal data misuse with strict thoroughness, the consumer of financial services must be supported by enhancing his/her financial literacy and digital competences. There is a significant volume of personal data that is collected and used by the financial institutions and the implications on the end user are considerable especially for those who are unaware of it or do not comprehend the financial services sector.

Financial sector is one the of the main sources of concern when analyzing the need of personal data protection as there are several elements that drew the attention to more care when establishing the level of personal data collected or stored, the range of analyses that offer insights on the individual or group trends or the extend of cybernetic exposure to privacy. Due to new technologies (continuous communications and multiple parties accessing personal data) and the global availability of the personal data, financial institutions have the moral and financial responsibility to offer protection of privacy, no matter the frequency and intricacy of interactions with their customer or different third parties. Especially after the pandemic, the responsibility to prevent and /or reduce the effects of data breach has become essential in order to retain the loyalty of the end user of financial services. All the regulation adopted in the privacy and personal data protection (such as OECD Consumer Policy Guidance on Mobile and Online payments, in 2014, OECD recommendation on consumer protection in e-commerce in 2016 and OECD G20 Toolkit for protecting digital consumers in 2018) have promoted the necessity to provide reasonable means to exercise the rights of the individuals and also the preoccupation for complementary actions such as financial literacy [8] . The role of national authorities entitled to investigate and correct the lack of compliance with the data protection law is essential as the need to provide expert advice for users and also for institutions as well as handle complaints has become critical. The increase in the awareness of personal data use and financial literacy is supported by several international groups, including OECD/INFE that has crystallized a framework of core competencies

required for the persons working or interacting with the financial sector [9]. The main directions of interest relevant for the financial services institutions in the area of personal data use are:

- Defending consumers against cyber-risks (such as phishing, data theft, ransomware, wire fraud) –more than 60% of global financial institutions were targeted by cyberattacks in 2022;
- Supporting vulnerable consumers to overcome the exclusion situation due to big and digital profiling [10] .

PERSONAL DATA IN FINANCIAL SECTOR

One of the concerns of the authorities (national and international) refers to the fact that the financial consumer is less and less aware of the volume of personal data that is being centralized by financial services providers due to increased online interactions, public information on social media or third parties (such as credit reference agencies/ insurance brokers a.s.o).

Pandemic has accelerated the rate of use of internet services and thus the use of online financial services – the year of 2022 recorded 5.3 billion users worldwide, meaning 66% of the global population, with China ordered first among the countries with the most internet users worldwide [11]. The impressive degree of Internet utilization is generating the collection of new personal data to be shared, analyzed and stored by third parties. The interconnectivity among devices is considered a second important source of personal data as more and more consumers are accessing the network of these objects and thus are contributing (sometimes without realizing it) to the collection of personal data – for example, telematics systems are responsible for collecting data on the destinations, behavior of the driver, incidents history; online banking application can draw conclusions on purchase patterns, investment habits; sources of income etc. Not all the Internet of Things devices allow the possibility to choose what to share with third parties and by failing to do that, those devices are becoming silent traders of data, in the background which brings about great exposures for the users of smart devices [12]. The privacy is no longer guaranteed as risk of hacking is high in this era of digital interactions at any time and consumers are lacking the knowledge to realize what data and how much time they are stored by the entities gathering information, under the premise that intend to offer tailor-made products. New types of personal data derive also from biometrics – either identity bodily or conduct features – the difficulty in these types of data arise from the fact that they cannot be easily modified or deleted if the risk of hacking occurs.

In a similar way to the progress of new types of personal data, there are significant developments in the area of analytical solutions that help predictive analysis in terms of patterns and correlations which, of course, are quite useful for financial institutions when establishing future income sources or expenses patterns/ behaviors of the customer. Among the best-known advances in the analytical capacities of the financial sector we may stress the following:

- Machine learning – development of algorithms used by computers to improve their performance based on the set of data they are fed. Regression and cluster analysis are the best destinations of this analytical tool;
- Profiling – the classification of individual consumers based on common elements – credit scoring, targeted advertising are examples of profiling;

- Data mining – technique that identifies patterns based on sets of data being analyzed.

The benefits brought by the sophisticated techniques are highly appreciated as a greater amount of personal data (non-necessarily financial) are being gathered by the financial service providers and may be used for future interactions with their customers, even though generalization does not work all the time.

The existence of regulatory provisions may trigger the use of one of the above tools (including the well acclaimed artificial intelligence) by the financial providers in different phases of the client relationship management process as may be noticed in Table 1 [2].

Function	**Type of personal data collected**	**Objective**
Customer profiling	Geolocation, purchasing habits, e-payments	Customer segmentation
Risk management	Credit information (credit scoring, big data, augmented analytics) Insurance information (activity sensors, physical activity tracker, telematics, home insurance, medical history)	Data aggregation in order to assess risks based on multiple sources
Robo-advice	Client needs, risk appetite	Personal financial plan (savings/investment)
Fraud detection	Continuous analysis of client spending	Almost instantaneous account management
Account aggregation	Banking account, investments, saving accounts	Personal financial management

Table 1. Functions and services of the financial providers making use of personal data
Source: author's representation of data

IMPLICATIONS FOR CONSUMERS OF FINANCIAL SERVICES

The increased use of personal data in the financial services has, without a doubt, major benefits for the consumers, if the financial consumer protection framework exists and is being complied with by the financial providers [13]. Moreover, the soundness of such decision is based on the hypothesis that the consumer is a digitally financial literate person – which, unfortunately, is not the case around the world [14].

Cheaper financial products, prompt offer to contract, increased competition due to the entry of FinTech companies, robo-advice, personalized products are some of the obvious advantages brought to the financial consumers – which seem to compensate the disadvantages generated by the privacy intrusion of a company [15].

The diversified offer of the financial providers due to the increased volume of personal data and complex analytical tools to process them may result in tailor-made offers which may be difficult for consumers to compare and understand, if their level of digital financial knowledge is low [16].

Digital financial literacy refers mainly to four categories of products and services that were also agreed by OECD to be critical in achieving for all the consumers, not only the most vulnerable ones [17]. The lack of understanding the products and services summarized in Table 2 increase the risk of understanding the way the use of personal data is carried out by the financial providers.

Type of financial product	Example
Payments	Electronic money, crypto-assets
Asset management	Mobile trading, crypto-assets training, robo-advisors
Alternative finance	Crowdunding, peer-to-peer lending
Other	Internet based insurance

Table 2. Types of new digital financial products
Source: author's representation of data

The applicable legal framework may decide the extend to which big data and machine learning may be used for profiling or risk management of the client, especially in the area of credit and insurance products. The data used in these instances may differ from personal data collected in the stage of Demands and Needs Analysis or may be collected without the customer being aware of the process, by inferring information on the customer based on similar customers' data, which may be detrimental for those vulnerable - for example in insurance, based on risk segmentation, some customers may be offered discounted rates while others may be rejected from insurance protection. Linking multiple sets of data and pieces of information is being possible with the help of the technological solutions and may be the cause of increasing the possibility of tracing non-identifiable data to individuals, thus improving the analytical capabilities of the financial providers and on the same time endangering the protection of personal data [18]. Due to this phenomenon, in credit sector, a customer may be analyzed not only on the base of credit scoring but also considering the buying habits (shops, products), the posts on the social media, the habits of their social contacts.

The way the new data are being used and analyzed, supported by the lack of regulation in some countries, may not be transparent enough for the customer, may lack the accuracy or the limitation in the access of data for financial institutions, thus disabling any dispute protection for the customer. These are the instances when a financial customer may find himself/herself in the situation of not knowing how to validate the negative decision or even how to better prepare for the following application.

The response of the financial customer to the benefits and risks generated by the use of big data is intriguing – if on the one hand the customer is aware of the exposure of their privacy, on the other hand they are willing to ignore this breach of privacy in order to receive better and cheaper financial products. Unfortunately, by accepting this trade, the customers remain oblivious to the terms and conditions of their data use in the financial industry.

Customers are concerned about their data may be misused and accessed by malevolent parties and also aware by the threats generated by cyber-risks – such as illegal access, theft of personal data, phishing, hacking a.s.o.

FINANCIAL LITERACY AND AWARENESS

2022 was the year when digital financial competencies were brought to light as the pandemic elevated the risk of financial losses for those vulnerable groups that missed both the digital and financial awareness. The effort to standardize the issue of digital finance and use of personal data in online financial services is still reduced in the majority of economies although several national projects have been implemented across Europe (Germany, Portugal, Spain) [19] .

Digital financial literacy became the star of the national strategies of financial supervisors as more and more cases of fraud, cyber-crime, ID theft are registered among the countries, especially for old people or for the young – vulnerable groups of the society with

limited financial resources. The concerns for understanding the personal data protection, the necessary precautions in case of online payments or the importance to notify the authorities in case of identity theft are already topics included in the Financial Literacy Programs for students or in public campaigns addressing the elderly people, vulnerable to electronic means of payment.

Moreover, the national authorities responsible for personal data protection are already in the process of adapting the national frameworks so that the customers have the knowledge of exercising their rights regarding the protection of their personal data or the limitations that must be obeyed by the international providers of services, including financial groups.

CONCLUSION

The latest trend in technological tools and the pandemic has brought about a significant development of the online financial sector offering quicklier, more-particularized services to the financial consumer. This objective meant also a demand of the financial providers to collect, analyze and store a wider range of personal data (not only financial), while complying with the adapted frameworks concerning customer protection and data protection.

Data breaches and cyber-threats determine the regulators and the financial institutions to pay more attention to the volume of data to be combined and stored and, in the same time, to enhance the awareness of the customer of the use of their personal data in the financial sector so that they may choose what to disclose, in case it is not necessary. The article presented the benefits and exposures from the perspective of the customer.

The effort to better calibrate the type and volume of personal data used in the financial sector must be dual – both from the part of the financial providers, that should pay attention to the limitations set by the regulatory framework, and the part of the customers, that should have a proactive approach in terms of personal data, understanding the reasons for sharing and implications of data analysis.

A coordinated effort of the financial regulators, data protection authorities and financial institutions in terms of digital financial literacy awareness programs may bring benefits on the medium term, based on the expertise of international forums such as World Bank or OECD, through its International Network on Financial Education.

REFERENCES

[1] B.Yuan, J.Li, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation," *International Journal of Environmental Research and Public Health*, volume *16*, issue 6,2019. [Online serial]. Available: https://www.mdpi.com/1660-4601/16/6/1070 . [Accessed Jan. 7, 2023].

[2] G.A.Teixeira, M.da Silva, R. Pereira, "The critical success factors of GDPR implementation: a systematic literature review," *Journal of Digital Policy, Regulation and Governance*, Volume 21, Issue 4, pp. 402-418., 2019. [Online serial]. Available: https://www.emerald.com/insight/content/doi/10.1108/DPRG-01-2019-0007/full/pdf?title=the-critical-success-factors-of-gdpr-implementation-a-systematic-literature-review . [Accessed Jan. 7, 2023].

[3] M. G. de Matos, I. Adjerid, "Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider," *Management Science* , 68(5):3330-3378, 2021. [Online serial]. Available: https://pubsonline.informs.org/doi/epdf/10.1287/mnsc.2021.4054 . [Accessed Jan. 8, 2023].

[4] R. Zhuo, B. Huffaker, S. Greenstein, "The impact of the General Data Protection Regulation on internet interconnection," *Telecommunications Policy*, Volume 45, Issue 2, 2021.[Online serial]. Available: https://www.sciencedirect.com/science/article/pii/S0308596120301737 . [Accessed Jan. 15, 2023].

[5] P.Oikarinen, "Pseudonymization of Personal Data with respect to the General Data Protection Regulation : A Telecommunications Industry Perspective", M. thesis, University of Helsinki, 2018. [Online]. Available: https://helda.helsinki.fi/handle/10138/235885. [Accessed Jan. 15, 2023].

[6] J. van Mil, J.P. Quintais, "A Matter of (Joint) control? Virtual assistants and the general data protection regulation," *Computer Law & Security Review*, Volume 45, 2022. [Online serial]. Available: https://www.sciencedirect.com/science/article/pii/S026736492200036X.

[7] Deloitte, "The time is now. The Deloitte General Data Protection Regulation Benchmarking Survey," 2017. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-benchmark-survey-report.pdf . [Accessed Feb. 3, 2023].

[8] OECD, "Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis," 2020. [Online]. Available: www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf. [Accessed Feb. 2, 2023].

[9] G20/OECD INFE, "Core competencies framework on financial literacy for adults," 2016. [Online]. Available: https://www.oecd.org/finance/Core-Competencies-Framework-Adults.pdf . [Accessed Feb. 2, 2023].

[10] Constrast Security , "Larger financial institutions hit by variety of cyberattacks in 2022," 2022. [Online]. Available: https://bankingjournal.aba.com/2023/02/larger-financial-institutions-hit-by-variety-of-cyberattacks-in-2022/. [Accessed Feb. 2, 2023].

[11] Statista, "Number of internet users worldwide from 2005 to 2022," January 30, 2023. [Online]. Available: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/. [Accessed Feb. 13, 2023].

[12] G. Rosner and E. Kenneally, "Clearly Opaque: Privacy Risks of the Internet of Things," 2018. [Online]. Available: https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd5. [Accessed Feb. 3, 2023].

[13] G20 OECD/INFE, "Policy Guidance Note on Digitalisation and Financial Literacy," 2018. [Online]. Available: https://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf . [Accessed Jan. 26, 2023].

[14] P. Morgan, B. Huang., L.Trinh "Minding the gaps in digital financial education strategies," November 24, 2020. [Online]. Available: https://www.g20-insights.org/wp-content/uploads/2020/11/minding-the-gaps-in-digital-financial-education-strategies-2-1606224578.pdf . [Accessed Feb. 2, 2023].

[15] GfK , "Willingness to share personal data in exchange for benefits or rewards - Global GfK survey," 2017. [Online]. Available: https://www.gfk.com/fileadmin/user_upload/country_one_pager/NL/images/Global GfK_onderzoek_-_delen_van_persoonlijke_data.pdf . [Accessed Jan. 26, 2023].

[16] Global Partnership for Financial Inclusion (GPFI), "G20 High-Level Principles for Digital Financial Inclusion, Global Partnership for Financial Inclusion," 2016. [Online]. Available: https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion. [Accessed Jan. 27, 2023].

[17] P.J. Morgan, B. Huang and L.Q. Trinh "The Need to Promote Digital Financial Literacy for the Digital Age. T20 Policy Brief," 2019. [Online]. Available: https://t20japan.org/policy-brief-need-promote-digital-financial-literacy/ . [Accessed Feb. 12, 2023].
[18] "Larger financial institutions hit by variety of cyberattacks in 2022," *ABA Banking Journal*, February 7, 2023. [Online]. Available: https://bankingjournal.aba.com/2023/02/larger-financial-institutions-hit-by-variety-of-cyberattacks-in-2022/ . [Accessed Feb. 12, 2023].
[19] World Bank, "Financial Literacy Survey Questionnaire. Washington," DC: World Bank, 2018. [Online]. Available: http://siteresources.worldbank.org/INTECAREGTOPPRVSECDEV/Resources/RU-WB-Financial-Literacy-Questionnaire.pdf . [Accessed Feb. 7, 2023].