AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
No. 1 (2023), pp. 22-27

APPLICATION OF CUSTOMER LOYALTY PROGRAMS AND ISSUES OF DATA PROTECTION

E. MAKSUTI, B. MAKSUTI

Eduina Maksuti[1], Bledar Maksuti[2]
[1]*Faculty of Technology and Business, Bedër University College, Tirana, Albania.*
https://orcid.org/0000-0002-6318-5466, E-mail: eduinamaksuti@gmail.com
[2]*The Prosecutor's Office of Tirana Judicial District, Tirana, Albania*

ABSTRACT

The business owners, administrators and managers are strongly depended on the internet, to develop their business. This fact is more obvious in cases when applying the loyalty programs and contacts with the customers. Marketers sometimes get lost in their business management and tend to be less focused on the legal issues, keeping their mind in the business growth. In this point, one of the key elements is being on compliance with the national and international legal norms of data protection of the customers. The relevant changes in the domestic law makes it more difficult for the business owners to operate their online marketing business. Nevertheless, it seems that such legal provisions with regard to privacy and data protection are not fully respected and the state institutions should do more about this. This article discusses the application of customer loyalty programs and the issues related to data protection, especially in Albania. It was found out that more efforts are needed to adhere to the EU standards in protecting personal data and certainly a stricter control by the government institutions is required on the way and methods the big companies collect, store and share the personal information of the customers.

KEYWORDS: customer loyalty, online marketing, data protection, legal issues**.**

INTRODUCTION

Customer loyalty programs (CLP), are a widely used marketing strategy that encourages customer retention and enhances sales. These programs offer customers incentives, discounts, and rewards for repeat purchases. While loyalty programs can be beneficial for businesses, they also raise important issues related to data protection.

Market analysis and customer segmentation are carried out by building profiles of individual customers based on their personal information, which customers supply to the vendor during enrolment to the loyalty program, and their purchase records, collected every time customers present their loyalty cards. The profiles thus assembled are used in marketing actions, such as market studies and targeted advertising (Blanco-Justicia, A., and Domingo-Ferrer, J. 2016).

With regard to the Albanian business reality, the issues of data protection, are relevant and remain a concern, despite the modern exiting legal framework that has been established to confront them. One of the most vulnerable points is the data obtained, data storage and data

protection. It seems that the majority of the personal information given willingly or not by the consent of the customers, is circulating form one business to the other or to better paraphrase it, the personal data transfer is a business on its own.

1. BENEFITS OF CUSTOMER LOYALTY PROGRAMS

Customer loyalty programs have several benefits for businesses. One of the main benefits is customer retention. Research has shown that customers who are enrolled in loyalty programs are more likely to make repeat purchases than those who are not (Kumar and Shah, 2019). Loyalty programs also help businesses gain insights into customer preferences and behaviour. By analysing the data collected through loyalty programs, businesses can develop marketing strategies and make informed decisions about inventory (Ramanathan, 2016).

Albania, being relatively new in the market economy after the political transition, has adopted new contemporary marketing strategies, but still there is a lack of experience and research in this field (Maksuti, 2022).

Nevertheless, the customer loyalty programs are becoming a growing trend and more and more companies are approaching customers using social network applications, emails, telephone numbers and other means of communications. This is a much more comfortable and convenient way for the marketers and administrators of the companies than developing some exhausting and "within legal complying" strategies.

1.1.ISSUES RELATED TO DATA PROTECTION

While customer loyalty programs can be beneficial for businesses, they also raise important issues related to data protection. One of the main concerns is the potential for data breaches and misuse of customer information. Loyalty programs require customers to provide personal information, such as their name, address, email, and phone number, as well as information about their purchasing behaviour. This information is typically stored in a central database that can be accessed by employees or third-party vendors, and is vulnerable to cyberattacks and other security threats (Dwivedi et al., 2019).

In addition, businesses may use customer data for purposes beyond the administration of the loyalty program. For example, they may use customer data for targeted advertising or share data with third-party partners. These practices can violate customers' privacy rights and erode trust (Nikou and Bouwman, 2019).

The inter-related growth in loyalty programs (LP) and big data applications increases the importance of the societal consequences that accompany the many benefits of this virtuous circle. While societal concerns would exist even in the absence of an LP, LPs have the potential to exacerbate these issues. Hence, it is important for firms and researchers to take societal concerns into consideration when designing and managing LPs to the benefit of all stakeholders (Stourm, et al., 2020).

Research has shown that data protection issues mostly violate the areas of inequality, privacy and sustainability with regard to customers' personal data.

The violation of inequality comes from the CLP data ability to mark consumers with a good quality of precision. The personal data can be processed to identify which types of customers could be targeted with particular offers or services, but such adapted marketing

schedules can also be easily implemented because the members are very reachable not only in the virtual way of speaking.

Firms are explicitly shifting resources away from non-participating customers in favour of customers who participate in their CLPs, which may lead to accusations of discriminatory customer treatment (Lacey and Sneath, 2006).

One of the main issues of invading on customer privacy is grounded on how personal data are gathered, stored, analysed, and shared. The use of high tech creates a huge database stationed on the companies' servers. Taking into consideration this aspect, CLPs implementation now collect more and data thus chasing customer's behaviour offline and online, including all available devices. Meanwhile sustainability is not strictly connected to the personal data protection it is worthy to mention that using customers' personal preferences of the CLPs succeed on changing consumption patterns. Clearly, individuals' consumption patterns not only change their own physical and mental health, for better or worse, but also affect those around them (Stourm et al., 2020).

1.2.PROTECTING CUSTOMER DATA

To address concerns related to data protection, businesses must take steps to protect customer data and ensure that their loyalty programs are transparent and compliant with relevant regulations. One way to protect customer data is to implement robust data security measures, such as encryption, access controls, and monitoring. Businesses must also provide clear and concise information to customers about how their data will be used and shared (Nguyen and Mutum, 2019).

Is is obvious that such initiatives are not and should not be taken by the companies or business owners. It is a matter of governmental institutions and customers' protection entities which somehow should push for the reinforcement of harsher legal provisions and penalties on case of infringement on privacy and personal data.

1.3.COMPLIANCE WITH APPLICABLE REGULATIONS

Businesses must also comply with applicable data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union. GDPR mandates strict requirements for data collection, processing, and storage. Businesses that operate in the EU or process data of EU residents must comply with GDPR.

Regarding the Albanian case, the Republic of Albania has established a complete legal framework for customer's protection including personal data protection. Concretely, it is the Law 9887/2008 "On protection of personal data" which provides;

1. "Personal data" shall mean any information relating to an identified or identifiable natural person. Elements used to identify a person directly or indirectly are identity numbers or other factors specific to his physical, psychological, economic, social and cultural identity etc.

2. "Sensitive data" shall mean any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as with data concerning his health and sexual life.

Besides this law, personal data protection is enforced by the provisions of the Albanian Criminal Code and the establishment of the institution of the Commissioner for the Right of Information and Protection of Personal Data.

2. DATA PROTECTION ISSUES, ALBANIAN CASES

One of the main problems occurring while using and CLP is the management of the data. In this point there are several issues to be addressed;

a. The sensitive data of the customers such as date of birth, profession, ID card number, phone number, e-mail address, home/work address etc.
b. The provider of the data in case it is not the customer itself but companies specialised in this field.
c. In marketing or application of CLP the frequency of using personal data for advertisements or even notifications.
d. Finally, and most importantly the protection of the personal data.

In a typical Albanian case, the unauthorised use of the personal data is quite a phenomenon that occurs in daily basis. This may happen by phone calls to advertise new products and emails from uncertified addresses.

Despite that fact that a special institution for the protection of personal data has been established namely the Commissioner for the Right of Information and Protection of Personal Data, few measures has been taken to prevent and stop such phenomenon.

It has to be mentioned that as recently reported by the prestigious Albanian Monitor", the Albanian Bureau of Insurance has been fined for providing personal data of people involved in accidents to the benefit of third parties in order to use them for taking financial benefits.

These are rare examples that are plausible and encouraging but in most common cases when customers ask the advertising companies, particularly people who call, "how did you find this number?", the most common answer is "from the large database that we have or from other companies where you have been registered".

Besides breaching the above-mentioned law no. No. 9887 dated 10.03.2008 "On protection of personal data" such disturbance constitutes a misdemeanour namely a criminal offence provided by the the Albanian Criminal Code article 275, "Malevolence use of phone calls", provides that "*Malevolence use of telephone calls made to disturb another's peace constitutes criminal contravention and is punishable by a fine or up to one year of imprisonment*".

In this regard the opinion of the lawyers is divided, some of them think that the unauthorised use of a customer's phone number, by calling him often does not constitute malevolence and could be resolved by a civil litigation, the other part of the scholars insist that if after several warning "not to disturb", the advertising company, keeps on calling, this action is considered as a breach of criminal law. Without entering in details of the legal procedure, let's consider it as a legal violation.

In most cases, it has been noticed that when a customer agrees to join a customer loyalty program, often, no prior contract of formal agreement is signed between parties for the protection of the personal data. While many employees hasten to attract more and more

customers, even the customers hasten to benefit from the offers and other privileges, thus forgetting to establish terms and conditions for the personal data protection.

In other cases, the contact between the company and customer is made through the cashier or via phone calls, the agreement of the customers for the use of the personal data is given not by signing a formal contract.

The biggest problem that is evident in most countries is the personal data provided by specialised companies that administer them mostly in an unknown way. Officially the personal data of people are administered by the state institutions and very big companies of social networks such as Meta (Facebook, WhatsApp, Instagram), email providers (google, outlook etc) where people by voluntarily registering, enter their personal information.

The issue in discussion is how the companies that provide personal data obtain such personal information when in most cases no customer has given them and based on what legal grounds do they offer to the interested companies.

With this regard a stricter control by the state institutions is needed to control the access that companies have on personal information of the customers.

CONCLUSIONS

In conclusion, customer loyalty programs offer a number of benefits to businesses, including increased customer retention and valuable insights into customer behaviour. However, the use of these programs also raises important issues related to data protection and privacy, which must be addressed through the implementation of strong data security measures and compliance with relevant regulations. By balancing the benefits of loyalty programs with the need to protect customer data, businesses can create a valuable marketing strategy that benefits both themselves and their customers.

Simultaneously, government bodies and customer protection entities should strengthen their efforts in applying laws and regulations in order to increase the efficiency of protection of the personal data.

In concrete terms, the designated governmental entities should protect the central databases where the personal information is stored, which can be accessed by employees or third-party vendors, and is vulnerable to cyberattacks and other security threats (Dwivedi et al., 2019).

Understandably a closer cooperation is needed between state and private companies which must also provide clear and concise information to customers and state entities about how their data will be used and shared (Nguyen and Mutum, 2019).

With regard to the Albanian case, more efforts are needed to adhere to the EU standards in protecting personal data and certainly a stricter control by the government institutions is required on the way and methods the big companies collect, store and share the personal information of the customers.

REFERENCES

1. Blanco-Justicia, A., and Domingo-Ferrer, J. (2016). Privacy-aware loyalty programs. Computer Communications, 82(1), 83–94.
2. Dwivedi, Y. K., et al. (2019). Blockchain: A panacea for healthcare cloud-based data privacy and security? Journal of Medical Systems, 43(8), 1-17.

3. Kumar, V., and Shah, D. (2019). Loyalty programs and their impact on customer retention: A study of the Indian retail sector. Journal of Retailing and Consumer Services, 50, 322-331.
4. Lacey, R., and Sneath, J. Z. (2006). Customer loyalty programs: are they fair to consumers? Journal of Consumer Marketing, 23(7), 458–464.
5. Law 7895/1995, Albanian Criminal Code [1995] as amended by the Law No. 146/2020, Official Journal 5, Art 275.
6. Law 9887/2008, "On protection of personal data" [2003] as amended by the Law No.120/2014. Official Journal 44.
7. Maksuti, E. (2022, September 15-16). The role of loyalty programs on customer loyalty in hotel industry: A five-star hotel case in Albania. REDETE: Ancona, Italy.
8. Nguyen, B., and Mutum, D. S. (2019). A review of customer loyalty programs in the hospitality industry: Lessons for the gaming sector. Journal of Hospitality and Tourism Management, 38, 107.
9. Nikou, S. A., and Bouwman, H. (2019). Online privacy violation: The influence of website interactivity and privacy assurance on users' personal information disclosure. Journal of Business Research, 96, 319-328.
10. Ramanathan, U. (2016). Big data analytics: a study of loyalty program data and decision-making. Journal of Business Research, 69(5), 1562-1566.
11. Stourm, V., Neslin, S.A., Bradlow, E.T. et al. (2020). Refocusing loyalty programs in the era of big data: a societal lens paradigm. Marketing Letters 31, 405–418.
12. V. (2022, September 21). Byroja Shqiptare e Sigurimit gjobitet për shkelje të ligjit për mbrojtjen e të dhënave personale. Revista Monitor. https://www.monitor.al/byroja-shqiptare-e-sigurimit-gjobitet-per-shkelje-te-ligjit-per-mbrojtjen-e-te-dhenave-personale/