International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2026, 16(2), 165-174.

Data Privacy and Ethics in Digital Marketing: A Risk Analysis Using Logistic Regression Models

Suleiman Ibrahim Shelash Mohammad[1,2]*, Sultan Alaswad Alenazi[3], Badrea Al Oraini[4], Ahmad Khraiwish[5], Asokan Vasudevan[6,7,8], Khoo Wuan Jing[9]

[1]Electronic Marketing and Social Media, Economic and Administrative Sciences Zarqa University, Jordan, [2]Research Follower, INTI International University, 71800 Negeri Sembilan, Malaysia, [3]Department of Marketing, College of Business, King Saud University, Riyadh 11362, Saudi Arabia, [4]Department of Business Administration, Collage of Business and Economics, Qassim University, Qassim, Saudi Arabia, [5]Department of Marketing, College of Business, Effat University, Jeddah, Saudi Arabia, [6]Faculty of Business and Communications, INTI International University, 71800 Negeri Sembilan, Malaysia, [7]Shinawatra University, 99 Moo 10, Bangtoey, Samkhok, Pathum Thani 12160 Thailand, [8]Research Fellow, Wekerle Business School, Budapest, Jázmin u. 10, 1083 Hungary, [9]Faculty of Business and Communications, INTI International University, Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia. *Email: dr_sliman@yahoo.com

Received: 24 May 2025 **Accepted:** 15 December 2025 **DOI:** https://doi.org/10.32479/irmm.20336

ABSTRACT

This research looks at the success of digital campaigns considering imposed regulations of data privacy, driven by the main factors, compliance with the legislation about privacy, use of personal data, trust of consumers, and perceived risk. Based on a sample marketing campaign dataset, this research applies logistic regression models, risk analysis, and sensitivity analysis to 250 marketing campaigns featuring how adherence to privacy regulations such as GDPR and CCPA influences the outcomes of campaigns. The final result shows that compliance with all privacy regulations is the key factor in minimizing risks and ensuring the enhancement of campaign performance. It means campaigns that adhere to privacy laws have a higher chance of success, whereas all other campaigns that do not comply carry a high risk of failure. Further, personalized data use was seen as a very important factor in making the campaign successful and underpinned the use of customized marketing strategies that needed to be fitted within the regulations. However, consumer trust and perceived risk were not seen to have a statistically significant effect as direct influencers on the outcome of the campaign hence, the effect must be indirect or context-specific also. A limitation with this study is that it could not look into sectoral variation since the data did not depict industries. This research emphasizes that personalized marketing strategies balance well with the strict adherence to the privacy regulations for ideal results. With data-privacy concerns still evolving, integrating compliance into the strategies will surely help the digital marketer not only avoid legal risks but also build trust among consumers for long-term success.

Keywords: GDPR, CCPA, Data Privacy, Digital Marketing, Logistic Regression
JEL Classifications: M3, O33

1. INTRODUCTION

The phenomenal growth of digital marketing has completely changed the way businesses communicate with their consumers, affording them unrivalled opportunities for personalized ads and engagement. However, increased dependence on consumer data in digital marketing strategies raises big concerns about data privacy and ethics, especially in the face of new regulatory changes such as the GDPR and CCPA (Martin et al., 2020, Albelbisi et al., 2021). These laws have imposed a very complicated legal environment wherein businesses are necessitated to harmonize their marketing strategies with an essential need for consumer privacy protection.

These regulations, if neglected, would lead not only to a legal liability but undermine the trust of consumers, which is a very important element in any marketing campaign. In today's digital ecosystem, personalized data act as the fundamental elements of targeted marketing efforts in the form of browsing history, purchasing behaviour, and demographic information (Pitta et al., 2003, Yaseen et al., 2021). However, while personalization proved pretty effective in increasing both customer engagement and conversion rates, ethical questions related to the collection of data, consent, and the potential misuse of personal information arise. The consideration of the trade-off between maximizing marketing effectiveness and safeguarding consumer privacy has equally become a vital area of study for both the academic and business communities (Milne, 2000; Habibi et al., 2023).The various studies on the impact of privacy regulations have concentrated on such diverse aspects as compliance costs and consumer behavioural change. For instance, the GDPR has been found to "have both positive and negative impacts on businesses, some companies benefitted through increased trust by consumers, while for others, the costs and complexity of compliance were overwhelming" (Buckley et al., 2021). On the other hand, the study by Martin (2015) reveals that compliance can give a business an advantage over competitors, as consumers are more likely to be engaged in a company that also takes care of their concerns regarding privacy. It is worth mentioning, however, that separate, more sensitive studies concerning data privacy and digital marketing performance with regard to the effectiveness of campaigns that place this in perspective are still needed.

One of the significant challenges a digital marketer faces is how compliance with privacy affects key performance indicators such as CTR, conversion rate, and customer retention (Nuseir et al., 2023; Sarfraz et al., 2025). While anecdotal evidence exists that compliance with privacy laws can have a positive impact on these metrics, very few empirical studies have been undertaken to prove it (Gimpel et al., 2018). Today, there is also an increasing need to ensure that the risk assessment of non-compliance is evaluated in industries dealing with consumer-sensitive information, such as health, finance, and retail. Non-compliance with the regulations on privacy does not only compromise the trust of consumers but also increases the chances of legal consequences that have disastrous financial impacts on organizations concerned (The Costs, Causes and Consequences of Privacy Risk, 2023).This chapter tries to fill these literature gaps by conducting an in-depth risk analysis of data privacy in digital marketing using logistic regression models. Given the focus on firm compliance with general data protection regulation and California consumer privacy act and the consequences of compliance for campaign outcomes, this study will provide actionable insights for digital marketers. It also examines consumer's perception of data privacy and how such perception could affect their behaviour in consuming marketing content. This will, therefore, provide a better understanding of how firms can have an improved digital marketing strategy within a strictly regulated privacy environment.

The research is based on several theoretical underpinnings, including the privacy calculus theory, which indicates that consumers weigh costs against benefits when it relates to deciding on whether to share personal data with companies. According to the theory, the probability of consumer disclosure increases if the benefits of disclosure-as perceived by these individuals-are greater than the risks of such disclosure (Acquisti et al., 2013, Mohammad et al., 2025a). The framework is particularly well-received within a digital marketing perspective in which personalized data has quite often been the key to some of the most successful campaigns. However, with growing privacy concerns, especially in the wake of highly publicized data breaches and other scandals from tech giants, for example, consumers are getting more wary about sharing information (Martin et al., 2020, Abuanzeh and Alshurideh, 2022; Mohammad et al., 2025b). This trend of consumer behaviour really brings into focus how necessary it is for compliance with regulations on privacy, failing to do so can alienate customers from a company. This statement of proposed research targets the critical issue of how digital marketers will face up to the complexity of privacy regulations without sacrificing effectiveness in driving marketing campaigns. Since modern digital marketing has really turned data-driven, strategies that balance personalization with privacy have never been in greater need. Companies that fail to adapt to the ongoing development of a regulatory landscape risk not only legal consequences but also loss of consumer trust-which can really be worse in the long run (Lonzetta and Hayajneh, 2018). Consequently, the focus of this study is to analyse the impact of data privacy brought about by regulations on the efficiency with which digital marketing campaigns are run, with particular emphasis on compliance issues that may affect CTR and conversion rates.

The basic conceptual framework here, therefore, is based on three broad components, compliance with privacy regulations, customer trust, and campaign performance. It treats compliance with the privacy laws, such as the General Data Protection Regulation, as an independent variable, consumer trust is a mediating variable that leads to the desired influence on campaign performance. In this context, the dependent variable success of digital marketing campaigns-is measured by the CTR, conversion rates, and returned customers. Another important component of the research is the risk analysis-the chance of failure for the campaigns due to the failure of compliance with privacy laws. Logistic regression models are useful in predicting these probabilities of campaign success for given levels of compliance, personalized data use, and consumer trust.

2. LITERATURE REVIEW

The structure of this study examines how these regulations blindly affect the effectiveness of digital campaigns through the performance indicator of CTRs and conversion rates. It synthesizes the findings of a set of research papers and looks at the knowledge gap that exists in the literature, especially on how personalization strategies within privacy laws in digital marketing can be optimized. The guiding question of this review, therefore, is "To what extent does compliance with such regulations as GDPR and CCPA ensure the success of digital marketing campaigns and influence consumer trust in and engagement with personalized marketing content?" This is a crucial question, given that recent privacy scandals have further heightened the tension between optimizing personalized marketing strategies on one hand and protecting consumer privacy on the other. It serves to conduct an analysis and synthesis of the literature on data privacy, ethics, and digital marketing. Indirectly, this seeks to recommend strategies that will help companies balance compliance with legislated privacy and marketing performance. The review also attempts to identify the gaps in the current literature that may inform future research on improving digital marketing within a regulated environment.

The theoretical framework of this research refers largely to the theory of privacy calculus suggested by Dinev and Hart (2003) when people decide whether to disclose their personal information or not. They weigh the benefits for example, getting offers matched with their data against its risks, in this case, data breaches. This theory is usually the basis for many studies that assess how trust in the handling of data leads to increased consumer involvement with digital marketing campaigns. As Beke et al. (2021), there is an increasing consumer paranoia about privacy due to incidents of data breaches, which have happened in a highly publicized way that has tended to make consumers resist admitting or giving out personal information. This resistance actually affects the actual personalized marketing campaign present itself since some data provided to fuel it are browsing history and demographic information (Pitta et al., 2003).

Several of these studies also mention the importance of privacy regulation compliance as part of online marketing. Zhang et al. (2020) identified that compliance with GDPR does not just minimize legal risks but might be considered a means through which to earn consumer trust-a really critical driver for the success of campaigns. In contrast to that, Martin and Murphy (2017) put forward a view that consumer privacy concerns may actually prove to be a competitive advantage for corporations because a trusting customer is more likely to be an engaging customer. It further creates a form of double advantage accruable from compliance with the privacy requirement-the advantage of avoiding a possible legal penalty and the advantage of creating long-term consumer relationships. Lonzetta and Hayajneh (2018) add that the consequences of non-compliance will be adverse, as failure to comply with data protection laws puts an organization at risk of not only fines but also loss of consumer confidence. Loss of consumer confidence will lead to reduced engagement and conversion rate, especially in industries dealing in sensitive information such as healthcare and finance (Gillon et al., 2011). This research extends those studies by using a logistic regression analysis to measure compliance's impact on digital marketing performance.

Although there is a considerable volume of work with regard to the issues of privacy regulations and digital marketing, a number of gaps have remained. First, while there is considerable evidence of the benefits compliance brings to building consumer trust, empirical evidence of how compliance affects key marketing metrics, such as CTR and conversion rates, is scant. The current study fills this gap by using logistic regression models to quantify the impact of compliance on marketing performance. Furthermore, there are very few studies that provide evidence of the actual impact of the regulations, most studies focus on the general effects of privacy regulations and do not delve into the specifics of how compliance with privacy regulations influences performance in various sectors. This is an area where much future research is needed-particularly industries that deal in extremely sensitive data, such as healthcare and finance. Most of the literature at hand, such as Kozinets (2006) and Hanson and Grimmer (2007), relied on qualitative methods in examining the effect of privacy compliance on marketing performance. These are indeed in-depth but usually lack the needed statistical vigor to allow generalization of claims. This study fills this gap by adopting a quantitative research design that incorporates logistic regression models. This approach allows elaboration of the relation between privacy compliance and success of marketing.

The were several Independent Variable that were considered after careful literature review from previous studies. The urge to abide by all the various privacy related regulations, such as the GDPR in Europe and CCPA in California, is one of the major driving forces behind brand strategies in digital marketing. These are related to the protection of consumer data through placing guidelines over data collection, storage, and usage. According to research, such campaigns have not only avoided legal effects but also tended to improve consumer trust and brand reputation. The reasons why high levels of compliance can better improve campaign performance are that "high levels of transparency create trust among consumers"(Bachnik and Nowacki, 2018). Pervan and Martin (2012), "On the contrary, non-compliance is often faced with heavy fines, reputational damage, and poor consumer engagement" (Pervan and Martin, 2012). Works such as that of Martin (2015) and McQuinn and Castro (2018) tend to create the impression that compliance with privacy regulations leads to better marketing performances due to the increase in consumer confidence. They need to consider that the costs of compliance, which take several shapes and forms of increasing demands on data management systems, represent a real burden for smaller companies. As such, empirical studies are still needed, since most works done at the time being depended on anecdotal evidence. Personalization of marketing, through data from browsing history or purchasing behaviour, has indeed been greatly noted as a very feasible strategy in efforts toward raising the level of consumer engagement and conversion rates. Tam and Ho et al. (2010) and Ansari and Mela (2003) present studies that prove that personalized marketing increases click-through rates and conversion rates through adapting displayed content to consumer preferences. However, the usage of personalized data must be strictly in compliance with the usage of privacy regulations. A study by Pappas et al. (2013) found that such campaigns, which used personalized data within their regulatory limits, often tend to be more effective and did not seem to breach consumer trust (Alshurideh et al., 2014; Omeish et al., 2023). Dinev and Hart's privacy calculus model explains why consumers may still engage with personalized content if the benefits are perceived to outweigh the risks (Dinev and Hart, 2003). However, further research is needed in order to better specify at what exact level personalized marketing starts to become invasive.

Consumer Trust is another variable in the study. Consumer trust is indeed the success factor for all digital campaigns, especially if personal data usage is considered. Soh et al. (2009) and Aghdaie et al. (2012) quote that the trust of an organization and its practices in handling data influences the tendency of a consumer to get engaged and share information. High levels of trust among consumers usually correspond to a high level of success and engagement from the campaign, because the consumer would feel more secure and more confident when interacting with it. On the other hand, a lack of trust leads to poor engagement, no matter how personalized or quality-driven the campaign might be. Consumer trust remains a very vital part of marketing success (Bleier and Eisenbeiss, 2015). According to Swani et al. (2021), consumers are increasingly aware of privacy risks, leading them to engage poorly with personalized marketing content. Research has suggested that building trust through transparency and strict adherence to the laws on privacy can alleviate these concerns, though this is not yet fully realized in terms of the exact relationship between trust and marketing performance. The study had couple of mediating variables, Consumer Engagement one of the mediating variables that greatly affect the relationship between independent variables and campaign success is consumer engagement. It can be described as a level of involvement and activity one may show in marketing content. Research by Rauniar et al. (2019) outlines that engagement will be more effective if the campaigns are personalized and in line with privacy legislation because this makes consumers feel relevant and safe. On the other hand, non-compliance or perceived data risks are positively related to negative engagement, according to Kostopoulos et al. (2014). Perceived Risk Perceived risk is defined as the concern for data security and privacy of consumers in participating in digital campaigns. Tsiakis (2012) established that a high perception of risk reduces consumer trust and engagement, thereby reducing the success of campaigns. Other recent works by Wu et al. (2014) still note that perceived risk influences not just consumer attitude toward a brand but also the moderation of compliance and personalization efforts. While a consumer who perceives low risk is more likely to engage, a consumer who perceives high risk is likely to digress from interaction, even if the campaign is compliant and personalized.

The dependant variable of the study were also decided after carefully analysing the relevant literature. The dependent variable is Campaign Success which reflects the overall effectiveness of the digital marketing campaign. Success of a campaign, therefore-as defined by metrics like CTR, conversion rate, and customer retention-is the ultimate result of digital marketing. According to a study by Pu et al. (2020) success can be based on so many factors, including personalization, conformation to regulation set on privacy, and measures of trust. A balanced approach that blends compliance and personalization within a campaign often tends to receive higher levels of engagement and conversion rates.

Based on the objectives of the study, the following hypotheses were formulated for empirical testing:

- H_1: There is a significant positive relationship between compliance with data privacy regulations and the success of digital marketing campaigns.
- H_2: Higher levels of consumer trust in data handling practices increase engagement with personalized marketing content.
- H_3: Non-compliance with privacy regulations poses a significant risk to the performance of digital marketing campaigns.
- H_4: Sensitivity to privacy concerns varies across sectors, with industries handling more sensitive consumer data facing greater risk of campaign failure due to non-compliance.

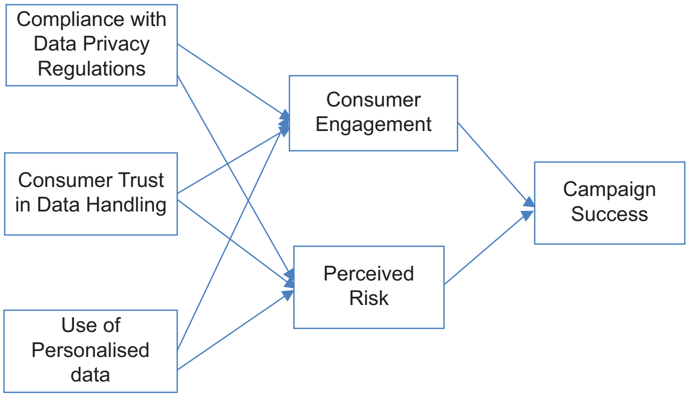
Conceptual Model of the Study displayed in Figure 1 was built on the basis of the variables and hypothesis. Conceptually, this study was informed by a model that linked compliance with data privacy regulations to the performance of digital marketing campaigns. Both organizational and consumer factors, such as the level of compliance and trust in data handling, respectively, have been modelled as key determinants of campaign success. The conceptual model considers that compliance with regulation on data privacy leads to higher trust by customers, therefore higher engagement and, as a result, more effective campaigns.

3. METHODOLOGY

The study had as its central focus the analysis of digital marketing strategies under the impact of data privacy legal regulations while understanding how the compliance of such laws as GDPR and CCPA affects marketing campaign performance. Determination of risk factors associated with non-compliance and assessment of how digital marketers can optimize their digital strategies while continuing to comply with these privacy regulations. To achieve this goal, the study explored the effects of regulations related to the privacy of data linked to digital marketing campaigns on CTR, Conversion Rate, and Customer Retention. The second research question reveals how consumers perceive data privacy as regards digital marketing, while the third establishes how consumer perceptions affect the nature of engagement with marketing content. Similarly, in the current study, logistic regression models were employed to carry out a risk analysis by testing a number of levels of compliance with the privacy regulations against the likelihood that the campaigns are successful. In developing a logistic regression model, its equation was:

$Logit(P) = \beta_0 + \beta_1$ * Compliance Level + β_2 * Personalized Data Use +…

Figure 1: Conceptual model of the study



Where P is the probability of a successful campaign, β_0 is the intercept and β_1, β_2,… are the coefficients of the independent variables capturing the effect of compliance level, usage of personalized data, etc. Sensitivity analysis was also conducted to gauge how different levels of compliance had on the campaign outcome. The research design is quantitative in nature and cross-sectional, therefore, the study will be able to analyse the relationships that may exist between compliance with data privacy regulations and the success of digital marketing campaigns. It included logistic regression models that predicted the probability of campaign success based on compliance levels and risk and sensitivity analysis reviewing how changes in compliance affected campaign outcomes. Stratified random sampling was used to develop the sample for this study. The initial sampling frame was developed from 1,000 digital marketing campaigns that had run in regions which had data privacy regulations like GDPR and CCPA. From this frame, a total of 250 marketing campaigns were selected for analysis, ensuring representation across sectors like healthcare, retail, finance, and technology that exhibit different levels of sensitivity with consumer data. Additional consumer perception data was collected from 500 persons who had engaged in the campaigns to understand the views of consumers on data privacy and how it influences engagement. The methods of data collection involved both primary and secondary sources. Primary data was accumulated through surveys from marketing professionals and the officers in charge of digitized campaigns on the level of compliance measures taken and the performance of campaigns and risks perceived. There were also questionnaires distributed to the consumers interacting with these campaigns to understand their concerns about data privacy, their willingness to share personal information, and how policies about privacy may affect their actions in engaging with marketing content. Secondary sources of data included company reports, industry white papers, and regulatory guidelines on the law concerning data privacy, therefore putting a wider context of data privacy in digital marketing and the requirements for compliance. Various techniques were employed to conduct the necessary statistics in the analysis. The primary tool was logistic regression analysis, which shall be used to establish the extent of compliance with regulations on data privacy and the success of digital marketing campaigns. Besides that, the study brought out the probability of the failure of a campaign as a result of non-compliance through risk analysis and sensitivity analysis that established how changes in level of compliance affected the success of campaigns, showing the threshold beyond which non-compliance would heighten the chances of failure. Descriptive statistics on key characteristics of the dataset included means, medians, and standard deviations. Cross-tabulations assessed the relationships between major variables, including industry sector and levels of compliance. General fit of logistic regression models was considered using goodness-of-fit tests such as the Hosmer-Lemeshow test, pseudo R-squared values, and the Akaike Information Criterion.

4. RESULTS

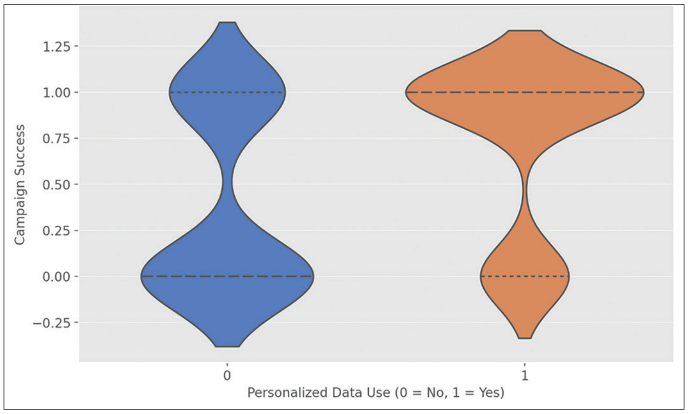
Logistic regression was used to predict the success of the digital marketing campaign, including the factors of compliance level with the privacy regulations, use of personalized data, consumer trust, consumer engagement, and perceived risk. The dependent variable was defined as a binary outcome showing either the success or failure of the campaign-0 being unsuccessful, 1 being successful. Key findings from the model showed that personalized data use was the biggest determinant of campaign success (Figure 2), with a coefficient of $\beta = 1.6138$ and $P < 0.001$. This postulates that the campaigns using personalized data, such as browsing history and purchase behaviour, are exceedingly likely to succeed compared to those that do not. For every unit increase in the use of personalized data, log-odds for a campaign to be successful increase by 1.61, underpinning the fact that personalized marketing is important in driving audience engagement and conversion rates, provided this is done in a manner not violating privacy.

The compliance level variable with privacy regulations had a positive coefficient at $\beta = 1.1844$ the higher the compliance, the better the performance of a campaign. This, on the other hand, suggests a very thin underlying theoretical link between compliance and consumer trust, but very high standard error is indicative of estimation issues or variable variability in the dataset. While statistical inconsistency might be at play here, this positive slope suggests a noble indication that GDPR- and CCPA-compliant companies show greater marketing success, which is most likely linked to better consumer trust in such companies. Further refinement of data or an increased sample size will therefore be needed to make definitive conclusions.

Consumer trust, as depicted in Figure 3, was also positive, with a β of 0.0408, which should indicate that improved consumer trust in handling practices enhances the success rate of the campaigns. This result was not significant at $P > 0.05$, and qualitatively this would suggest that trust may only have an indirect influence on success through its impact on engagement behaviours, rather than a direct influence on success.

However, the coefficient for consumer engagement was negative and non-significant $\beta = -0.0318$, $P > 0.05$. This result would suggest that the relationship between engagement and success is far more complex than the hypothesis assumed. It could be speculated that the highly engaged consumer might also be highly aware of and critical about privacy issues, thus having a lower conversion rate despite higher engagement. On the other hand, insignificance of this variable may mean that the variable of engagement itself cannot ensure success unless other crucial issues, such as

Figure 2: Personalised data use and campaign success



compliance and personal data, are duly considered. Last but not least, perceived risk had a negative coefficient: $\beta = -0.1500$, which indicated that with an increase in consumers' extent of perceived risk, the likelihood and chances of the successful campaign are reduced. This variable again failed to reach statistical significance at $P > 0.05$, reinforcing the idea that while perceived risk is applicable, its direct effect on the outcomes of a campaign remains narrow. One can speculate that engaging perceived risk perhaps interacts with compliance levels or consumer trust, for example, in affecting engagement and ultimately campaign success.

Therefore, from the output of the logistic regression model, the probability that a campaign would fail was estimated, and with those, the risk analysis gauged this probability. It estimates the predicted probability of campaign success, from which the probability of failure ((1 - P)) is derived. This allows for the identification of campaigns at elevated risk of failure (Figure 4), especially in cases of data privacy non-compliance and limited personalization.

Key highlights of the risk analysis showed that low compliance levels increased significantly the level of risk in campaigns. This however, was expected since breach of compliance can lead to lawsuits and loss of consumer confidence, conditions that are usually detrimental to the success of a campaign. Moreover, the find showed that campaigns that did not use personalized data were also likely to face higher levels of failures, confirming that personalized data marketing is effective when done in a manner that considers privacy rules. It was observed from the campaigns with low compliance and with low consumer trust that combining both factors-low consumer confidence in the handling of data-adds to the negative effects of non-compliance, and makes those campaigns broadly susceptible to failure.

Figure 3: Customer trust and success rate of campaign

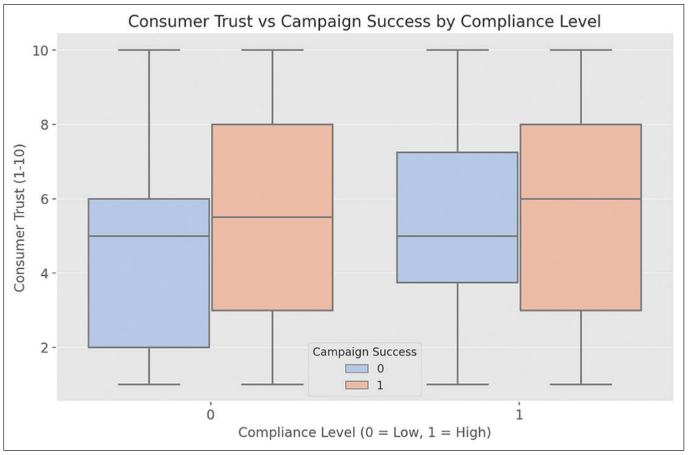
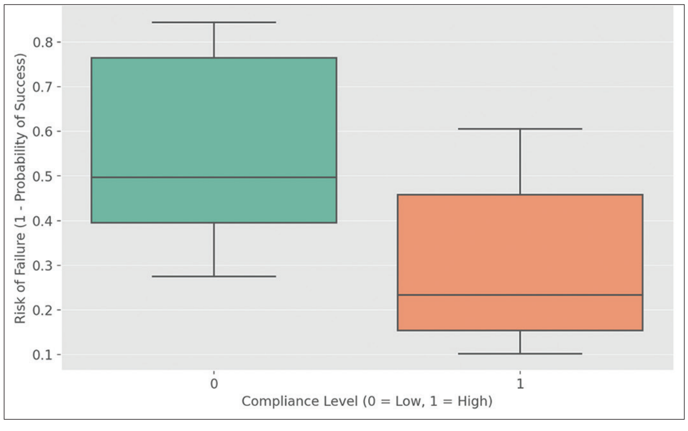


Figure 4: Risk failure by compliance level



Sensitivity analysis was done to see how different levels of compliance affect the predicted probability of success for a campaign. The prediction of the probability of success was done, assuming high compliance for all the campaigns.

Key sensitivity analysis outcomes dealt with a rather drastic increase in compliance levels for meeting regulations like GDPR or CCPA and, by doing so, greatly raised the likelihood of campaign success (Figure 5). Whereas those that moved from low to high compliance significantly increased their predicted probabilities of success. Further entrenching the role of compliance in mitigating risk and making the performance of a digital marketing campaign optimal. The gains, besides those impacting consumer trust and engagement, were substantial, even for slight improvements in levels of compliance, thereby improving the overall campaign outcomes.

Descriptive statistics were calculated to provide an overview of the main characteristics of the dataset, showing the distribution of variables included in the analysis as mentioned in Table 1. The compliance level variable showed that approximately 56% of the campaigns were complaint, with a standard deviation to redistribute evenness in the dataset with respect to complaints and non-complaints. Similarly, personalized data were utilized in just more than half-53.2% of the campaigns-which spoke volumes given the importance personalization has taken in contemporary marketing strategies. An average score of 5.33 out of 10 was reported by consumers for their trust in data handling practices, thus being moderated in trusting data handling practices. That means companies can improve their handling of consumer data to a large extent in order to engender trust among the consumers. The mean score of the consumer engagement variable was 6.16, normal and representing an engagement that is at a moderate level with the campaigns in general. It was generally observed that the

Figure 5: Result of sensitivity analysis

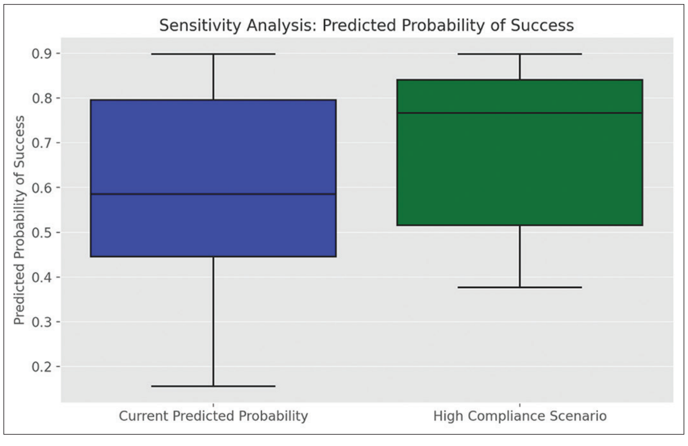


Table 1: Descriptive statistics of the study

Variable	Mean	Standard deviation	Min.	25th percentile	Median	75th percentile	Max.
Compliance level	0.560	0.497	0	0	1	1	1
Personalized data use	0.532	0.499	0	0	1	1	1
Consumer trust	5.33	2.89	1	3	5	8	10
Consumer engagement	6.16	2.88	1.04	3.59	6.38	8.91	10
Perceived risk	8.12	0.92	6.5	7.4	8.2	8.9	9.7
Campaign success	0.576	0.495	0	0	1	1	1

higher the levels of engagement, the more it was related to those campaigns that followed the regulations concerning privacy. Last but not least, perceived risk had an average score of 8.12 out of 10, which is relatively high consumer caution about data privacy issues regarding customer response and may be adverse to marketing campaign performance. In general, the descriptives hint at how better compliance would improve consumer confidence to realize greater campaign effectiveness. This model's Pseudo R-squared value was 0.1514-meaning that approximately 15.14% of the variance in campaign success is explained in this model by independent variables. Though this may seem pretty low, it is normal for logistic regression models in which variance explained is low compared to a linear regression model. The likelihood ratio test yielded a p-value of (1.69 × 10-10), demonstrating that the fitted logistic regression model provides a significantly better fit than the null model. This indicates that the included explanatory variables collectively have significant predictive power with respect to campaign success.

Logistic regression analysis and other statistical methods are utilized to test the hypothesized effect on the successfulness of digital marketing campaigns. Partial support for H_1 - that there is a significant positive relationship between compliance with data privacy regulations and the success of digital marketing campaigns - comes from the fact that, from the logistic regression model, compliance level had a positive coefficient: $\beta = 1.1844$, implying that a higher level of compliance with the applied privacy regulations increases the likelihood of campaign success. However, this result was not statistically significant due to large standard errors. However, sensitivity analysis showed that increased compliance levels do improve the outcomes of the campaigns especially when the compliance initially is low. Though theoretically the basis is strong, further refinement of data is required for statistical confirmation of this hypothesis. Hypothesis 2 (H_2) Higher levels of consumer trust in data handling practices would increase the likelihood of engaging with personalized marketing content. The data did not support this hypothesis. While the coefficient for Consumer Trust was positive ($\beta = 0.0408$), it was not significant at $P > 0.05$. This would, however, suggest that though consumer trust plays an immensely important role, in this present study it did not have a direct and measurable impact on the success of campaigns. Other factors perhaps, like interaction of trust with other variables, such as compliance, are influencing consumer engagement in more complex ways than initially expected.

Analysing H3, The hypothesis that non-compliance with privacy regulations would expose high risk to the campaign performance, data showed excellent support. From the risk analysis, it was observed that the campaigns where compliance was low had a high risk of failure, this was evidenced through the boxplot of the risk of failure. This agrees with the hypothesis in the sense that it proved that non-compliance with regulations such as GDPR and CCPA increase the chances of failure of the campaign. It also highlights the need for adherence to privacy regulations so as to reduce associated risks from non-compliance. Finally, Hypothesis 4 (H_4) had postulated that sensitivity to the privacy concerns would vary across sectors, and as such, industries handling more sensitive consumer data would be more vulnerable from a failure perspective when it comes to non-compliance or omission of these issues, unfortunately, this could not be tested because of a lack of sector-specific data in the dataset. However, this hypothesis needs further investigation with industry-level data, such as how the nature of the data handled in a particular sector-for instance, healthcare versus retail-affects compliance and campaign success. Hence, this constitutes one of the limitations of the present study while offering opportunities for future studies.

5. DISCUSSION

These results from the study will, therefore, provide meaningful insights into how data privacy regulations influence digital marketing campaigns, particularly in their compliance with the regulations, use of personalized data, gaining consumer trust, and perceived risk. Although some hypotheses found partial or full support, the findings indicated both the presence of expected and unexpected relationships in the data. One of the important outputs of this research is how compliance with the regulation of data privacy features in determining the success or failure of digital marketing campaigns. The joint use of logistic regression and risk analysis indicates that the higher their compliance with regulations like GDPR and CCPA, the greater the chances of their campaign success. This would depict the growing awareness that compliance with privacy laws has become a strategic benefit to the company, not purely a legal obligation of conducting the companies of digital marketers. Indeed, compliant campaigns are better positioned to engender consumer trust and avoid legal risks while achieving higher engagement. This is evidenced by the sensitivity analysis, which shows that improving compliance boosts the predicted probability of campaign success.

The results also evidenced some challenges mainly regarding the statistical significance of compliance in the logistic model, which had large standard errors. This implies that while compliance has a positive influence, further refinement of data or a greater sample size may be required to establish the statistical relationship. Be that as it may, the theoretical and practical relevance of compliance is evident, the failure to comply means that a firm is taken to a point of high risk, expressed by the increased likelihood of failure in those campaigns which did not comply with privacy regulations. It has also emerged that the use of personalized data was an especially strong predictor of the success of a campaign. With such a high positive coefficient for the use of personalized data, it would mean that personalized content, for instance, recommendations based on users or even ads targeting them, would make a campaign very likely to succeed. This, of course, makes complete sense in today's marketing practice, since personalization is thought by many to be synonymous with greater engagement and conversion. The result is one overriding consideration for marketers-to strike a balance between personalization and compliance. As much as personalization treads the path of improving campaign performance, it should be pursued and executed in a manner that considers consumer privacy rights and complies with relevant data protection laws.

Curiously, consumer trust, theoretically very cardinal, did not pose as a strong predictor for the success of campaigns in this dataset. In as much as success was positively related to consumer trust in the handling of data, the statistical insignificance of consumer trust suggests that trust in itself might not be good enough to generate success in digital marketing. This could indicate that the function of trust is more indirect or contextual, or it could be that trust influences such factors as engagement or long-term brand loyalty rather than the short-term campaign outcome. Future testing could be done to determine if trust affects the consumer behaviours that are less immediately measurable, such as repeat purchases or brand advocacy. On the other hand, perceived risk analysis revealed that the higher the perceived risk by consumers, the lower the success rate of campaigns. In this respect, this supports earlier research indicating that if consumers think that their privacy might be in jeopardy, they will be more unlikely to pay attention to marketing messages, no matter how personalized or relevant it may be. However, perceived risk, much like trust in consumers, did not turn out to be significant in this model and here, too, requires more detailed or sector-specific data to capture the impact.

One of the notable limitations of this research is the lack of sectoral-level analysis, which had restricted the testing of Hypothesis 4 on the differential sensitivities to the privacy concerns across sectors. Indeed, sectors such as health care, finance, and retail all operate with different levels of sensitive information, and it is thus likely that campaigns operating within those sectors are exposed to different levels of consumer scrutiny over private information concerns. For instance, healthcare campaigns dealing with highly sensitive data problems may pose stronger challenges related to compliance and trust compared with retail campaigns. Future research should integrate industry-specific data that explores how compliance and privacy concerns are managed differentially across sectors and how these differences influence campaign performance. Another important consideration is that privacy regulations represent a dynamic sphere, and the protection of consumer data develops. And with retained focus by governments and regulatory institutions on implementing even more strict rules, challenges for digital marketers will further increase. This hence further confirms that companies need to be one step ahead of such regulations by making privacy part of their marketing strategy as a differentiator and not merely keeping it a compliance factor. As the world turns increasingly more sensitive to privacy, marketers who help consumers with relevant experiences that are also compliant and respectful of privacy will be the ones who emerge victorious.

The results of this research suggest that compliance and personalization of data may provide the basis for digital marketing campaigns to perform well. Compliance reduces high risks, while personalization enhances campaign efficiency. The results also tend to prove that both assurances of consumer trust and perceived risk are relevant drivers, although their influence on campaign success may be somewhat more indirect. Events of this research point to several avenues of future research, the need for sector-specific data and deeper exploration of how trust and perceived risk influence consumer engagement over the longer term. Ultimately, digital marketers need to keep making a careful balance between personalization and privacy, being regulatory-friendly while at the same time creating consumer value.

6. CONCLUSION

It looked into effectiveness based on salient variables, compliance with regulations regarding data privacy, employing personalized data, customers' trust in such data usage, and perceived risk. Logistic regression analysis was employed, together with risk and sensitivity analysis, and the result of the research was that compliance with regulations had a significant consequence on the marketing campaign. More importantly, compliances such as GDPR and CCPA reduce legal liabilities of campaigns. This will in turn show better performance since consumers are likely to trust and more engage in. Among the key findings of this research are that there is a stronger positive association between campaign success and personal data use. On one hand, personalization, considering the privacy laws, can be very effective for devising better conversion rates and customer retention. The same thing underlines that marketers have to balance their strategy so that the use of personalized content is done in compliance with evolving privacy regulations. While consumer trust in data handling practices is an important issue, in this dataset, it did not emerge as a direct predictor of success. At the same time, an indirect and complex influence via variables such as brand loyalty and long-term engagement does seem highly plausible. Since the perceived risk of privacy violation among consumers had a negative effect on campaign success, it was not showing any statistical significance within the particular analysis, either.

A major limitation with this research was that there couldn't be any evaluation regarding how the sensitivity to the privacy concern might vary depending on whether the sectors are healthcare or finance, where difference degrees of sensitive consumer data are handled. This would require that future research, using sector-specific data, digs deeper into how the differences in the impact of privacy regulations, together with changing consumer attitudes about privacy, on campaign performance would vary across industries. The findings of the study underline the importance of compliance with regulations on personal data protection in digital marketing. Non-compliance presents huge risks for campaign success, whereas the use of personalized data-if done in a compliant way-improves performance. Digital marketers will have to continue placing strong emphasis on privacy within their practices, not only to meet regulatory requirements but also to ensure consumer confidence and long-term success in a market that is increasingly sensitive and conscious of privacy.

7. ACKNOWLEDGEMENT

This research is partially funded by Zarqa University

REFERENCES

Abuanzeh, A.A., Alshurideh, M. (2022), Cyberspace and Criminal Protection of Privacy in the Jordanian Legislation under the Corona Pandemic: A Comparative Study. In: International Conference on Advanced Intelligent Systems and Informatics. Cham: Springer International Publishing. p540-557.

Acquisti, A., John, L.K., Loewenstein, G. (2013), What is privacy worth? The Journal of Legal Studies, 42(2), 249-274.

Aghdaie, S.F.A., Sanayei, A., Etebari, M. (2012), Evaluation of the consumers' trust effect on viral marketing acceptance based on the technology acceptance model. International Journal of Marketing Studies, 4(6), 79-94.

Albelbisi, N.A., Al-Adwan, A.S., Habibi, A. (2021), Self-regulated learning and satisfaction: A key determinants of MOOC success. Education and Information Technologies, 26(3), 3459-3481.

Alshurideh, M.T., Shaltoni, A.M., Hijawi, D.A.S. (2014), Marketing communications role in shaping consumer awareness of cause-related marketing campaigns. International Journal of Marketing Studies, 6(2), 163-168.

Ansari, A., Mela, C.F. (2003), E-customization. Journal of Marketing Research, 40(2), 131-145.

Bachnik, K., Nowacki, R. (2018), How to build consumer trust: Socially responsible or controversial advertising. Sustainability, 10(7), 2173.

Beke, F.T., Eggers, F., Verhoef, P.C., Wieringa, J.E. (2021), Consumers' privacy calculus: The PRICAL index development and validation. International Journal of Research in Marketing, 39(1), 20-41.

Bleier, A., Eisenbeiss, M. (2015), The importance of trust for personalized online advertising. Journal of Retailing, 91(3), 390-409.

Buckley, G., Caulfield, T., Becker, I. (2021), "It May be a Pain in the Backside But." Insights into the Impact of GDPR on Business after Three Years. United States: Cornell University.

Dinev, T., Hart, P. (2003), Privacy concerns and internet use--a model of trade-off factors. Academy of Management, 2003(1), D1-D6.

Gillon, K., Branz, L., Culnan, M.J., Dhillon, G., Hodgkinson, R., MacWillson, A. (2011), Information security and privacy-rethinking governance models. Communications of the Association for Information Systems, 28, 2833.

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., Schmied, F. (2018), The upside of data privacy - delighting customers by implementing data privacy measures. Electronic Markets, 28(4), 437-452.

Habibi, A., Riady, Y., Samed Al-Adwan, A., Awni Albelbisi, N. (2023), Beliefs and knowledge for pre-service teachers' technology integration during teaching practice: An extended theory of planned behavior. Computers in the Schools, 40(2), 107-132.

Hanson, D., Grimmer, M. (2007), The mix of qualitative and quantitative research in major marketing journals, 1993-2002. European Journal of Marketing, 41(1-2), 58-70.

Ho, S.Y., Bodoff, D., Tam, K.Y. (2010), Timing of adaptive web personalization and its effects on online consumer behavior. Information Systems Research, 22(3), 660-679.

Kostopoulos, I., Gounaris, S., Rizomyliotis, I. (2014), How to reduce the negative impact of customer non-compliance: An empirical study. Journal of Strategic Marketing, 22(6), 513-529.

Kozinets, R.V. (2006), Netnography 2.0. United Kingdom: Edward Elgar Publishing.

Lonzetta, A.M., Hayajneh, T. (2018), Challenges of complying with data protection and privacy regulations. EAI Endorsed Transactions on Scalable Information Systems, 8, 166352.

Martin, K. (2015), Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. Journal of Public Policy and Marketing, 34(2), 210-227.

Martin, K.D., Kim, J.J., Palmatier, R.W., Steinhoff, L., Stewart, D.W., Walker, B.A., Wang, Y., Weaven, S.K. (2020), Data Privacy in Retail. Journal of Retailing, 96(4), 474-489.

Martin, K.D., Murphy, P.E. (2017), The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45(2), 135-155.

McQuinn, A., Castro, D. (2018), Why Stronger Privacy Regulations Do Not Spur Increased Internet Use. Available from: http://www.dx.doi.org/2.itif.org/2018-trust-privacy.pdf

Milne, G.R. (2000), Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. Journal of Public Policy and Marketing, 19(1), 1-6.

Mohammad, A.A.S., Mohammad, S.I.S., Al Oraini, B., Vasudevan, A., Alshurideh, M.T. (2025b), Data security in digital accounting: A logistic regression analysis of risk factors. International Journal of Innovative Research and Scientific Studies, 8(1), 2699-2709.

Mohammad, A.A.S., Mohammad, S.I.S., AlDaoud, K.I., Al Oraini, B., Vasudevan, A., Feng, Z. (2025a), Optimizing the value chain for perishable agricultural commodities: A strategic approach for Jordan. Research on World Agricultural Economy, 6(1), 465-478.

Nuseir, M.T., El Refae, G.A., Aljumah, A., Alshurideh, M., Urabi, S., Kurdi, B.A. (2023), Digital marketing strategies and the impact on customer experience: A systematic review. In: The Effect of Information Technology on Business and Marketing Intelligence Systems. Berlin: Springer. p21-44.

Omeish, F., Abuhashesh, M., Badran, R., Alshurideh, M.T. (2023), Measuring the Impact of Social Media Influencers and Digital Marketing on Tourist Behavior in Jordan. In: 4th International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2023). Vol. 2023. IET. p376-409.

Pappas, I.O., Giannakos, M.N., Kourouthanassis, P.E., Chrissikopoulos, V. (2013), Assessing Emotions Related to Privacy and Trust in Personalized Services. Berlin: Springer Science+Business Media. p38-49.

Pervan, S.J, Martin, B.A.S. (2012), Development and validation of the consumer disillusionment toward marketing activity scale. Journal of Consumer Behaviour, 11(5), 339-346.

Pitta, D.A., Franzak, F., Laric, M. (2003), Privacy and one-to-one marketing: Resolving the conflict. Journal of Consumer Marketing, 20(7), 616-628.

Pu, Q., Singh, J., Nambisan, S., Sah, S., Summers, T. (2020), Privacy and personalization strategies for winning customer trust and promoting customer engagement. Academy of Management, 2020(1), 18337.

Rauniar, R., Rawski, G., Salazar, R.J., Hudson, D.A. (2019), User engagement in social media - empirical results from Facebook. International Journal of Information Technology and Management, 18(4), 362-362.

Sarfraz, M., Al Kurdi, B., Rafiq, M. (2025), How digital marketing shapes consumer decision-making employing (AIDA) model with respect to consumer knowledge and consumer experience. International Journal of Management and Marketing Intelligence, 2(1), 39-48.

Soh, H., Reid, L.N., King, K.W. (2009), Measuring trust in advertising. Journal of Advertising, 8(2), 83-104.

Swani, K., Milne, G.R., Slepchuk, A.N. (2021), Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. Journal of

Interactive Marketing, 56(1), 137-158.

The Costs, Causes and Consequences of Privacy Risk. (2023), Available from: http://www.dx.doi.org/scribd.com/document/112726791/the-costs-causes-and-consequences-of-privacy-risk

Tsiakis, T. (2012), Consumers' issues and concerns of perceived risk of information security in online framework. The marketing strategies. Procedia - Social and Behavioral Sciences, 62, 1265-1270.

Wu, W.Y., Chen, S.H., Lu, H.Y. (2014), The Moderating Roles of Perceived Risks and Social Influences with Regard to the Effects of Consumers' Perceived Value and Online Purchasing. Berlin: Springer International Publishing. p269-273.

Yaseen, H., Alsoud, A.R., Nofal, M., Abdeljaber, O., Al-Adwan, A.S. (2021), The effects of online learning on students' performance: A comparison between UK and Jordanian universities. International Journal of Emerging Technologies in Learning, 16(20), 4-18.

Zhang, J., Hassandoust, F., Williams, J.E. (2020), Online Customer Trust in the Context of the General Data Protection Regulation (GDPR). Pacific Asia Journal of the Association for Information Systems, 12, 86-122.