

Article

Not peer-reviewed version

Protection Of Personal Data In The Context Of E-commerce

[Zlatan Morić](#)*, [Vedran Dakić](#), [Daniela Đekić](#), [Damir Regvart](#)

Posted Date: 7 August 2024

doi: 10.20944/preprints202408.0480.v1

Keywords: personal data; GDPR; e-commerce; advertising; marketing



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

Protection of Personal Data in the Context of E-Commerce

Zlatan Moric *, Vedran Dakic, Daniela Djekicand and Damir Regvart

Algebra University, University of Zagreb, 10000 Zagreb, Croatia

* Correspondence: zlatan.moric@algebra.hr

Abstract: This paper examines the impact of stringent regulations on personal data protection on customer perception of data security and online shopping behavior. In the context of the rapidly expanding e-commerce landscape, ensuring the security of personal data is a complex and crucial task. The study of several legal frameworks, including Malaysia's compliance with EU regulations and Indonesia's Personal Data Protection Law, provides valuable insights into consumer data protection. The challenges of balancing data safeguarding and unrestricted movement and tackling misuse by external entities are significant and require careful consideration. This research elucidates the pivotal role of trust in e-commerce environments and the deployment of innovative e-commerce models designed to minimize personal data sharing. By integrating advanced privacy-enhancing technologies and adhering to stringent regulatory standards such as the GDPR, this study demonstrates effective strategies for robust data protection. The paper contributes to the academic discourse by providing a comprehensive framework that synergizes legal, technological, and procedural elements to fortify data security and enhance consumer trust in digital marketplaces. This approach aligns with international data protection standards and offers a pragmatic blueprint for achieving sustainable data security in e-commerce.

Keywords: personal data; GDPR; e-commerce; advertising; marketing

1. Introduction

Online stores in Croatia have become more popular due to the global COVID-19 pandemic and the closure of physical stores. The exposure and protection of personal data online hinders the rapid adoption of faster Internet services. The number of online retailers is increasing due to enhanced consumer safety measures. Therefore, safeguarding the personal information of individuals who use the Internet, particularly those who engage in online shopping, is increasingly crucial.

This study investigated the potential impact of more stringent data protection regulations on enhancing online shopping security for customers in Croatia. The author sought to determine whether implementing more stringent regulations would enhance Internet safety by evaluating respondents' subjective perceptions, users' familiarity with the rules, and indicators of secure websites. The data was collected through an anonymous survey using Google Forms, which consisted of 33 questions across various categories. Data on gender, age, environment size, computer literacy, Internet security, and online shopping behavior were gathered. The survey was administered between September 1 and 10, 2023, to a sample of 100 individuals.

The research data was analyzed using Microsoft Excel. The findings are visually represented through graphs, illustrating respondents' attitudes and subjective impressions regarding personal data protection, vulnerability, and shopping habits. These graphs compare the data before and after the implementation of stricter regulations. The analysis also considers factors such as education, computer literacy, age, and other relevant data.

Data privacy is a significant concern in e-commerce, with various challenges and solutions explored across multiple studies. Arora [1] highlights the difficulties in protecting consumer data amidst the growing popularity of e-commerce platforms. This study underscores notable privacy

breaches and the need for stringent government regulations to safeguard personal information. Future research should focus on evolving legal frameworks to address emerging threats.

Muneer et al. [2] discuss privacy and security threats in e-commerce, emphasizing the need for technical solutions to mitigate risks. The paper suggests that without eliminating these threats, consumer trust will falter. The authors call for further investigation into innovative privacy protection techniques and enhanced consumer awareness strategies.

Boritz and No [3] review the trade-off between necessary data disclosure and privacy risks in e-commerce. They observe that much of the research is outdated and fails to consider recent technological advancements. Future studies should address these gaps, examining the implications of new technologies on e-commerce privacy.

Ghani and Sidek [4] analyze how personal information is utilized in e-commerce and the associated privacy risks. They argue for stricter control measures to prevent misuse. The authors recommend further research into advanced encryption methods and developing comprehensive privacy policies to protect consumer data better.

Salim and Neltje [5] explore the legal protection of personal data in e-commerce transactions, using Indonesia as a case study. They identify significant legal gaps and advocate for implementing a comprehensive data protection bill. Future research should evaluate the effectiveness of such legislation in different jurisdictions.

Moore and Dhillon [6] question the efficacy of privacy seals in building consumer trust in e-commerce. Many websites lack privacy statements, and abuses continue despite self-regulation efforts. The authors suggest future studies should explore mandatory privacy legislation and its impact on consumer trust.

Zhong and Wang [7] review current issues of consumer privacy leakage in e-commerce and propose technological and legal solutions. They highlight big data's challenges and call for future research into developing robust privacy protection technologies and legal standards to mitigate these risks.

Farah and Higby [8] discuss the conflict between e-commerce data collection needs and consumer privacy. They highlight the limited success of self-regulatory initiatives and suggest the need for legislative action. Future research should focus on the impact of privacy laws like those in the EU on the profitability of e-commerce firms.

Antoniou and Batten [9] propose new models to enhance consumer trust in e-commerce by protecting personal information. They identify the cost implications for sellers and deliverers but suggest that increased consumer trust offset these. Future studies should compare the effectiveness of these models against traditional protocols.

Bella et al. [10] introduce a paradigm balancing anonymity and trust to enforce privacy in e-commerce. They critique existing protocols and propose a differential privacy-preserving function. Future research should explore the practical implementation of this new paradigm and its impact on consumer behavior.

Budiono et al. [11] explore consumer legal protection against defaults in e-commerce transactions in Indonesia. They identify gaps in the current legal framework and suggest that protections must be preventive and repressive. The paper advocates for better legal measures to handle disputes and calls for future research to focus on the effectiveness of these legal protections in practice.

Gadjong [12] examines the legal relationship and protections between service providers and consumers in personal shopping services via e-commerce platforms. The study highlights that service providers can be held accountable if consumers suffer losses due to non-fulfillment of legal obligations. It emphasizes transparent communication and fulfilling obligations such as compensation or product replacements. Future research should explore the effectiveness of these legal protections and the role of government regulations in ensuring a fair e-commerce environment.

Lu [13] explores the computer e-commerce security system in the context of big data. The study identifies critical security threats and vulnerabilities in e-commerce platforms, emphasizing the need for comprehensive security measures. The paper discusses the importance of data encryption, secure

payment gateways, and robust authentication mechanisms to protect consumer data. It suggests that future research should focus on developing advanced security technologies and implementing big data analytics to predict and prevent security breaches in e-commerce systems.

Saeed [14] argues that understanding customer reservations and perceptions of security and privacy in e-commerce applications is crucial for developing appropriate policies and secure technological infrastructures. Data collected in this paper was collected through an online questionnaire and analyzed using SmartPLS software and the partial least squares method. Research indicates that customers' perceptions of online data security and trust in e-commerce applications are influenced by factors such as credit card usage, information security, motivational factors, trustworthiness, and reputation.

Monsalve-Obreque et al. [15] proposed a microenterprise solution to standardize processes and improve competitiveness in a demanding market. The methodology is based on quality management and customer satisfaction principles for e-commerce. It aims to identify both internal and external failures to prevent issues and achieve satisfactory outcomes. The proposed modifications seek to improve user experience, simplify purchase and payment procedures, bolster support for computer microenterprises, and fortify data security and privacy. This study on national-level quality regulation facilitates the formulation of recommendations for other microenterprises and the establishment of protocols for B2C electronic commerce transactions.

Duarte et al. [16] argue that Generation Z is poised to become the dominant consumer demographic in the future. Their research sought to ascertain Generation Z's receptiveness to e-commerce in Portugal. This study employed a questionnaire to gather data, focusing on a conceptual model developed by reviewing existing literature. The dimensions were examined utilizing SmartPLS 4 and IBM SPSS Statistics 26. The results either confirmed or refuted hypotheses about trust, perceived risk, ease of use, attitude, usefulness, intention to use, privacy, and security.

Feedback data from a study by Chen et al. [17] has the potential to undermine user privacy by exposing buyers' identities and preferences, resulting in a significant number of users refraining from providing ratings. They also present ARS-Chain, a robust reputation-sharing framework for e-commerce platforms that utilizes blockchain technology to ensure security. The experimental findings demonstrate that ARS-Chain improves user privacy and preserves system performance, influencing trust mechanisms in e-commerce platforms.

A study by Burlacoiu [18] examines the specific attributes of electronic commerce in European Union nations amidst a pandemic, utilizing data from Eurostat Digital Economy for 2019-2020. Principal Component Analysis (PCA) of 27 variables unveiled additional dimensions that facilitate more convenient visualization. Clustering techniques reveal the presence of four distinct groups of countries exhibiting unique online commerce patterns that necessitate attention from government and business entities. Despite experiencing substantial growth, Romania's share of total retail in Southeastern Europe's e-commerce industry remains relatively low, although it is considered a significant player in the region. Utilizing models from other nations can facilitate Romania's progress toward achieving the level of success seen in advanced e-commerce economies.

A study by Kim [19] investigates the factors that motivate and impede online shopping on open-market platforms. A hierarchical regression analysis was performed on the response data collected from 417 Korean consumers to conduct a thorough investigation. The findings consistently demonstrated the influence of motivational factors on purchasing intention. Statistically, privacy concerns related to time-saving, perceived ease of use, and security concerns related to cost savings were found to moderate e-commerce concerns.

In their 2022 paper, Marjerison et al. [20] employ the Use and Gratification (U&G) theory to investigate the acceptance of AI-based chatbots in online shopping among Chinese consumers. Data analysis reveals that practical factors such as the "authenticity of conversation" and "convenience," as well as hedonic factors like "perceived enjoyment," contribute to positive attitudes towards Chatbots. Nevertheless, the acceptance of this technology has been impeded by concerns regarding privacy and the lack of technological maturity.

This paper is organized as follows. The next sections provide basic information about protecting personal data on the Internet. Then, we move to how an online store in Croatia works from the consumer and owner perspective before discussing how those two perspectives merge as we try to do digital marketing in e-commerce. We'll also cover legal frameworks like GDPR and ePrivacy in that section. The section after that contains the practical part of our paper, exploring the association of stricter regulations with data sharing. The last sections of our paper include topics related to future research areas and conclusions.

2. Protection of Personal Data on the Internet

Data protection refers to the entitlement of every individual to safeguard their privacy and avoid the misuse of their data to the owner's disadvantage. Every organization and entity that possesses an individual's data shall make that data available for scrutiny by the owner of said data. Every person should clearly understand the specific data an organization collects and how it manages it. Furthermore, individuals must be able to amend erroneous information and, in rare circumstances, have the option to erase it.

The Personal Data Protection Agency (AZOP) is an autonomous and sovereign governmental entity created by the Personal Data Protection Act in the Republic of Croatia. The Agency's objective is to enforce Regulation (EU) 2016/67, which safeguards individuals' data processing (General Data Protection Regulation). It carries out duties within the boundaries and authorities set by the Act on the Implementation of the General Data Protection Regulation ("Official Gazette," No. 42/18), which guarantees the execution of the General Data Protection Regulation. The primary responsibility of the Agency is to educate stakeholders and the general public about the significance of safeguarding personal data and their associated rights and obligations. Additionally, the Agency is tasked with suggesting initiatives for professional development and training of personal data protection officers and overseeing the execution of all administrative and professional duties outlined in the General Regulation and the Act on Implementing the General Data Protection Regulation.

AZOP is a legally recognized organization with governmental authority that has a defined framework, financial resources, administrative leadership, jurisdiction, responsibilities, and specific activities and functions that it can carry out. Upon the Croatian Parliament's request, the Agency provides yearly reports analyzing the protection of personal data, data regarding the extent to which citizens' rights are respected in the collection of personal data, and measures issued by the law, which encompass all procedures.

The Agency's official website provides explicit information regarding the rights of data subjects, the data they have submitted, and the procedures for managing incorrect or incomplete data. The Personal Data Protection Act stipulates the criteria for collecting and processing personal data. Furthermore, it is ascertained which data is prohibited from being gathered and under what exceptional circumstances it may be collected. The law outlines the authority of the collection manager to designate a processor, specifies their responsibilities, sets the timeframe for the use of specific data, determines the types of data that the controller may or cannot disclose, and establishes the circumstances for transferring personal data overseas. Fines are assessed for contravening the terms of this law.

2.1. Basic Personal Data Concepts

The United Nations Universal Declaration of Human Rights, adopted on December 10, 1948, explicitly states that individuals should not be subjected to arbitrary intervention in their personal life, family, residence, or private correspondence or attacked on their reputation and honors.

Regarding safeguarding personal data, it is essential to note that personal data refers to any information that can be connected to an actual individual and, as a result, can be identified. Personal data can be categorized into three main types: primary, unique, and biometric. Basic personal data often includes information such as the individual's first and last name, residential address, date of birth, and other relevant details. Particular data encompasses information about an individual's race, nationality, religion, political party affiliation, participation in different associations, and similar

characteristics. Biometric data includes each individual's physical characteristics and behavioral patterns, which may be used to establish their identity quickly. Personal data includes physical attributes such as fingerprints, DNA, and personal photographs. In behavioral patterns, personal data refers to characteristics such as gait, vocal tone, accent, handwriting, facial expressions, and more.

As stated by AZOP, any organization, enterprise, or government entity handling personal data must provide stakeholders with clear and concise information regarding data utilization.

- The purpose for which your data will be used;
- The legal basis for processing your data;
- The duration for which your data will be stored;
- The parties with whom your data will be shared;
- Your fundamental data protection rights;
- Whether your data will be transferred outside the European Union;
- Your right to file a complaint;
- How do you withdraw your consent if given?
- The contact information of the organization/company responsible for processing your data.

A primary inquiry for this paper was to ascertain the level of familiarity among respondents regarding the concept of personal data and their willingness to disclose their data to a third party to conduct online transactions.

Data is intentionally and willingly acquired when gathering information at an online business. This information is provided by individuals who independently enter it to complete the online order form during registration. Standard information often includes the individual's first and surname name, street address with house number, zip code, city, country, telephone number, email address, and username.

Customers who have knowingly and willingly shared personal data have the right to request written information from the controller regarding the purpose of the data processing, the specific types of personal data being processed, and the expected duration of storage. Furthermore, the purchaser is entitled to rectify or modify personal information if it is found to be inaccurate, outdated, or incomplete. To accomplish this, it is imperative to notify the controller or customer service of any modifications.

Suppose the controller contains inaccurate information, such as the buyer's address or phone number. In that case, the customer's shipment may not be delivered electronically or sent to the erroneous address, harming the customer.

Each customer has the right to have their data erased, also known as the "right to be forgotten." They can make this request to the controller if any of the following conditions are met:

- Personal data is no longer necessary for collecting or processing purposes;
- The consent for processing the data has been withdrawn, and there is no other legal basis;
- An objection has been made to processing personal data, and the controller has no legitimate reason to continue processing it;
- The data has been processed unlawfully;
- The data was collected in connection with the offer of information society services;
- The controller is obligated by Union or State law to erase personal data to comply with a legal obligation.

The general workflow of an online shop and how the data moves through its subsystems is shown in Figure 1:

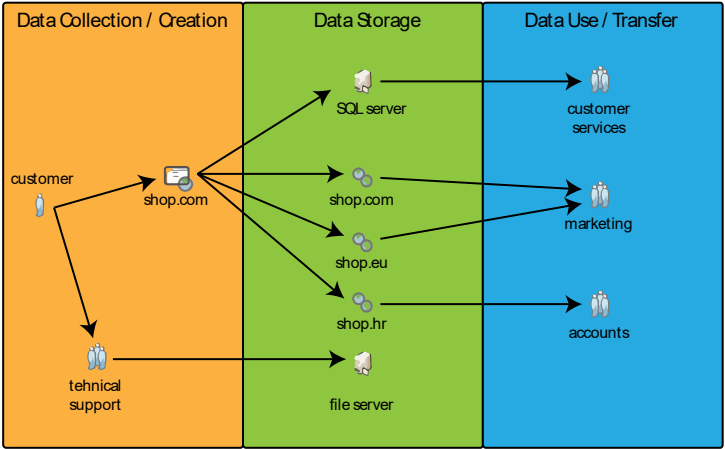


Figure 1. An online webshop data workflow example.

When setting up a user account to make an online purchase, many websites offer the option to write a review for the bought product. When users provide feedback on the product, the website gathers data such as comments, usernames, customer network addresses, information about the Internet browser, operating system, and similar details. As a result of the factors above, there is a potential for finding a link to a webshop when searching for an individual’s full name on an Internet search engine. This link may appear due to misrepresentation of someone else’s name or the deliberate choice of the user not to have their personal information displayed in search results. In such instances, every individual is entitled to reach out to the controller, such as Google, to formally request to remove a hyperlink from search results that includes personal information.

2.2. *GDPR*

As stated by the AZOP, GDPR is a regulation of the European Union that regulates uniformly the principles of personal data processing, the rights of data subjects, and the obligations of the controller and processor, as well as the organization of the personal data protection system in the procedural and institutional sense. The Regulation is a European regulation in terms of legal force above national laws and replaces the former Personal Data Protection Act in the Republic of Croatia. In addition to the GDPR, the organization and scope of the independent supervisory authority in the Republic of Croatia are governed by the Act on the Implementation of the General Data Protection Regulation (OG 42/2018). Although declared in May 2016, it did not take effect to its full extent until May 2018.

It is essentially a law that aims to protect the privacy and personal data of all citizens of a Member State of the European Union. Two changes are necessary to adapt the GDPR and the right to be forgotten RTBF, right to be forgotten). The very purpose of the regulation was to provide all stakeholders with insight and control over the use of their data from a third party. Therefore, the law aims to protect the data of all residents of the European Union. Still, all organizations that contact these same residents by collecting data, doing business, or providing them with services, wherever in the world, must be harmonized.

As stated in the introduction to this paper, the purpose of this paper was to determine whether there is an impact of adopting a stricter regulation of personal data protection on the perception of customers about the increased security of their data and, if any, whether security has encouraged customers to make more frequent purchases. To explore this, in the practical part of the paper, respondents were asked a set of questions that tried to determine how much their general knowledge of GDPR is, how vital Internet security is in general, and what data they are willing to share to purchase the desired product or service via the Internet. Following the answers given in this set of questions, a parallel was drawn between the habits and awareness of customers about safety itself before and after the regulations, and a conclusion was reached as to whether this ultimately resulted in more frequent purchases.

2.3. The Importance of Protecting Personal Data on the Internet

The value of personal data is increasing daily, due in part to its significance in marketing endeavors and because of instances of misuse and unlawful activity. The business outcomes of an advertising service company are directly influenced by the quantity and precision of its data. Prominent examples of this include Google and Facebook, which are industry leaders that have effectively eliminated most competitors in the Internet advertising sector. The influence of the quantity of high-quality personal data on the effectiveness of advertising campaigns surpasses that of traditional advertising channels like television, radio, or newspapers. Safeguarding personal data within information systems has become a paramount social concern and assumes a significant function.

Negligently handling individuals' data can significantly harm the rightful owners, infringing upon fundamental human rights about privacy. Leaking personal data can lead to several damaging consequences, such as the fraudulent use of the data to enter into detrimental contracts on behalf of others, the unauthorized withdrawal of significant sums of money from bank accounts, and other similar risks. Distinct economic models exist, including the Personal Information Management System (PIMS). Users can handle their personal information through a personal data management system rather than disclosing it to firms that sell it. Users who lack the time or requisite technical expertise can delegate this duty to specialized companies. Initially, it functions to transfer data between companies that engage in similar activities. However, it distinguishes itself because service providers primarily focus on monetizing their clients' data. In contrast, providers of personal information management services have a contractual obligation to safeguard the confidentiality of the data.

2.4. Collecting Confidential Information Online

The Internet is the most appropriate and widely utilized platform for gathering and examining personal data. Global interconnection substantially enhances communication and enables the utilization of many services, irrespective of the service provider's geographical location.

Multiple methods exist for organizations and enterprises to gather data, but a few fundamental ones include:

- Soliciting data as a prerequisite for delivering a service;
- Monitoring behaviors using cookies and comparable mechanisms;
- Acquire data from an external or independent source.

The current era is marked by the rise of several online services offered by different providers, including free email, cloud storage, social networks, and similar platforms. Most service providers require sharing personal data, including first and last name, date of birth, gender, and other relevant information, as a prerequisite for using their services. Despite the appearance of being free, the service comes at a significant cost, specifically in the form of personal data. Service providers are a crucial source of profits and income, yet they may appear minor to most end consumers.

Furthermore, several companies, including those beyond the Internet, employ comparable strategies. An exemplary illustration of this phenomenon can be observed in sweepstakes, loyalty programs, and other similar mechanisms that necessitate the provision of substantial personal data in exchange for a specific discount or the chance to win a reward. By examining an individual's name and surname, it is feasible to scrutinize their behaviors, including their purchasing behavior, such as the items and services they buy, the days they make purchases, the quantities they purchase, and the areas where they make their purchases. The abundance of data provides a remarkable foundation for conducting business analysis, ultimately enabling organizations to increase sales and broaden their presence in the market.

The above approaches yield nearly equivalent results when monitoring habits through cookies and other scripts. However, compared to the quantity of data gathered through earlier methods, the potential here expands significantly. Not only does it leave a trace through the IP address used to access it, which can quickly reveal the user's current location, but it also creates a database of devices

used to access services. This database includes information about the operating systems used by the users, the frequency and duration of their access, and details about the content or items they view. The abundance of data collected provides a more comprehensive understanding of the user than most individuals realize. The process of directly gathering user information is called “first-party” data. Seemingly harmless surveys can serve as a potent means of collecting personal data. While the information provided by respondents may appear innocuous and anonymous at first, when combined with data such as an IP address, it no longer remains anonymous. While the primary objective of “first-party” cookies is to enhance the user experience on a website, they can serve as a helpful analytics tool.

Companies’ most valuable data is collected through “first-party” methods. These methods obtain data at minimal cost, are easy to collect, and comply with regulations since the source and data generator are known.

The data referred to as the “other side” is classified as “first-party” data, which is collected by a different entity. Upon initial examination, the situation appears similar. However, it is essential to note that in this scenario, companies purchasing such data frequently lack insight into the data collection methods and compliance with regulations during the collection process. Additionally, there is a potential risk of data overlap. This is exacerbated by the constant accumulation of extraneous (i.e., trash) data by the same dataset, resulting in the need for significant resources for both analysis and storage. Another essential benefit of utilizing “third-party” data is the ability for organizations to expand their customer base by reaching out to new clients. This capability is not possible with their own “first-party” data.

Understanding the term “Third-party” data is crucial. It’s a collection of information from various sources consolidated into a comprehensive database. This data, essentially a compilation of numerous “first-party” data, is often purchased from an intermediary. Due to their large size, these databases are frequently organized and classified based on many factors and criteria. This allows companies to precisely ascertain the specific sector and type of data they intend to purchase, empowering them with the knowledge to make informed decisions.

The data collection landscape is changing thanks to increasing awareness and the implementation of new legislation like GDPR. Many major corporations now publicly declare they are discontinuing “third-party” data collection, mainly obtained from accompanying or tracking cookies. This shift is a reassuring step towards better data privacy and security.

Aside from the aforementioned lawful means of gathering data to construct customer and user databases, an illicit entity’s objective is to acquire individuals’ personal information for unlawful intentions. Most of these techniques can be classified as social engineering, in which the attacker manipulates the victim by posing as a helpful individual, a reputable organization, or a public institution, among other disguises.

Some prominent techniques of social engineering include:

- Phishing refers to the fraudulent practice of attempting to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising oneself as someone else;
- Vishing refers to a fraudulent activity in which individuals attempt to deceive others over the phone to obtain sensitive information or money;
- Smishing refers to fraudulent activity where scammers use text messages to deceive and manipulate individuals into revealing sensitive information or performing actions detrimental to their security.

Phishing, a form of computer fraud conducted through email, is a sophisticated deception commonly employed on behalf of an organization to deceive individuals into divulging personal information. The name is taken from the English term “fishing,” which metaphorically refers to the act of an attacker (fisherman) luring and capturing a victim (fish). This style of fraud is typically executed with a high level of sophistication, making it challenging to detect as a malicious attempt. It often entails luring users to a fraudulent website that resembles the legitimate organization’s site, frequently through a link in an email. This information should make us all more cautious and vigilant about our online interactions.

This attack has sub-variants, such as smishing, which involves using text messages to carry out a similar attack, and vishing, which requires phone calls. All the attacks above are classified as social engineering, in which the attacker effectively assumes a false identity, typically expressing concern for the victim's property or data safety. Subsequently, unsuspecting victims willingly disclose sensitive information. These attacks, known as data breaches, pose significant risks to businesses, resulting in substantial financial and reputational losses due to the exposure of sensitive information.

Aside from the techniques mentioned earlier in social engineering, which involve the attacker directly targeting the victim, several indirect ways of data theft exist. These include the creation of counterfeit websites, the unauthorized acquisition of databases, the procurement of stolen personal information through illicit means, and numerous more approaches. Computer programs obtained from untrustworthy sources containing embedded dangerous code, such as malware and spyware, present a significant threat as they are specifically designed to harm the user and illicitly gather data.

2.5. Identity Theft

Identity theft involves illicitly using another individual's personal information to engage in fraudulent activities, deceit, and impersonation for criminal purposes. The Internet serves as the primary platform for most identity theft cases. Identity theft is fraudulently assuming someone else's identity, typically to obtain financial or other advantages. Vidas defines identity theft as the act of appropriating someone else's identity without their awareness or permission. Identity theft occurs when somebody else uses our personal information.

The primary perils associated with identity theft are tangible harm and the ruin of the victim's reputation. The most prevalent forms of identity theft involve the unauthorized use of individuals' documents, such as identification cards, credit cards, and passports, as well as personal information, including names, addresses, unique registration numbers, and other pertinent details. The Internet provides an ideal environment for criminal activity due to the combination of carelessness, convenient access to personal data, and the ability for attackers to operate from a remote location. One issue stems from all Internet users being compelled to relinquish their data to different Internet services to access and utilize them. The increasing normalization of sharing personal information has made users less vigilant and more casual, reducing their caution towards the possible risks associated with data theft. Consumer negligence considerably aids data thieves, whether they exploit weak security measures of other parties or create a fraudulent replica of a popular Internet service's website. Identity theft can occur without the direct theft of personal information, as individuals often unknowingly expose themselves to risk by willingly sharing personal data on social networks.

3. Online Store in Croatia

An issue facing online businesses in Croatia is the comparatively low Internet adoption rate among the population. Based on the 2019 annual study from the e-business foundation, Croatia has a relatively low Internet usage and access rate of only 69% among its population. This positions Croatia near the bottom among the Member States of the European Union. Simultaneously, a mere 47% of Internet users in Croatia engaged in online purchases. The primary factors that lead individuals to avoid online purchasing include concerns over the security of payment transactions, doubts about the reliability of delivery and product replacement, and the potential for encountering issues when filing complaints about services or items. Based on this research, the primary mode of payment is through mobile devices, constituting 61% of all online payments. Card payments come next, accounting for 22% of transactions, while the remaining transactions use bank transfers, gift cards, and similar methods [21].

Advocates of digital technology often argue that traditional media, such as newspapers and television, will be replaced by their online counterparts as the primary sources of news and information. Furthermore, there is a prevailing notion that a similar scenario will unfold between brick-and-mortar stores and online retailers. However, while it is conceivable that all of the possibilities above may come to pass, the author maintains that these predictions will only materialize in the remote future. Multiple factors contribute to this issue, mainly a lack of adequate education

and understanding regarding modern technologies and a society prioritizing traditional customs and behaviors.

Most Croatians lack trust when making card payments online. The Association of Croatian Web Retailers has developed a solution to assist customers, known as the national trust label eCommerce Croatia Trusted Shop.

The trust mark is granted to any member who fulfills the ten conditions outlined in their code of conduct, expressly:

- A legitimate legal corporation backs the webshop;
- You know the specific items, time, and location of your purchases;
- The item you purchase is the item you receive;
- The prices are transparent and comprehensive;
- Payment is secure;
- The delivery information is easily understandable and provides all the necessary details;
- The entitlement to the option of returning the merchandise within 14 days.
- Complaints are promptly and equitably treated;
- Customer privacy is ensured;
- The displayed reviews are authentic.

The code of conduct is based on customer expectations and aims to enhance their confidence in the online store.

Individuals who shop online tend to have a greater propensity to purchase things with a limited lifespan and lesser quantities. For instance, consumer electronics dominate online purchases. Conversely, the proportion of clients purchasing vehicles, furniture, substantial household appliances, and similar items is far smaller when compared to traditional stores. The rationale is partly because these things are challenging to inspect in person without visiting a brick-and-mortar store. Conversely, the likelihood of one of the acquaintances possessing the desired mobile device, laptop, or similar technology is far greater than a refrigerator. One of the reasons for purchasing goods in smaller volumes is the ease of reclaiming them, as it is far simpler to return tiny items such as devices, books, and clothing. Online stores are used not only for purchasing things but also for buying numerous tickets, travel arrangements, and other services obtained through intermediaries rather than directly from the service providers.

Recently, there has been an apparent increase in the popularity of food ordering and delivery platforms. These platforms, such as Pauza, Glovo, and Wolt, are gradually replacing traditional fast-food restaurant leaflets. They offer the convenience of ordering and selecting food from various restaurants. The proliferation of these services has led to a scarcity of fast-food restaurants offering their delivery and direct ordering, instead relying on platforms of this nature.

3.1. Advantages and Limitations of Online Commerce

Upon examining the advantages offered by the online store for both individual and corporate users, it becomes evident that they are plentiful and often outweigh the drawbacks associated with this method of shopping. Customers are now liberated from the necessity of selecting multiple stores within a shopping area, which they must physically visit at a designated time. They have access to a diverse selection of stores where they can easily search for things based on specific criteria, see reviews from other customers regarding the quality of the desired items, and use this information to make informed purchasing decisions. Intense rivalry in online commerce often leads to price wars, as traders frequently operate with slim profit margins to acquire a more extensive consumer base. Thanks to its advanced level of automation, the Internet business does not adhere to traditional working hours, which is one of its significant benefits over conventional trading. One important benefit is the convenience of shopping from the comfort of your own home, which allows you to avoid traffic congestion and the hassle of finding parking. This alone is sufficient reason to opt for this sort of shopping. Research has indicated that online customers frequently exhibit distinct characteristics compared to traditional consumers since they are more inclined to seek respite from boredom through online buying. This discovery is especially pertinent to the trend of online buying

habits during free time. The absence of the need to travel or be physically present in a specific area to make a purchase is a crucial advantage of online stores since it allows for a wide range of choices. The capacity to select from a vast array of stores and commodities, irrespective of the seller’s geographical location, spans numerous cities and countries. Naturally, these factors contribute to intense competition among different establishments, benefiting the end customer through improved offers and more advantageous costs. In addition, the online product catalog offers the convenience of quickly searching and finding the needed item, which is a crucial feature for saving valuable time.

The convenience of having numerous stores accessible with just a few clicks enables effortless and rapid comparison of product offerings and prices across different stores. This increases the likelihood of customers obtaining their desired items and facilitates potential savings that may be overlooked when shopping at brick-and-mortar stores. Privacy during shopping and the absence of obligatory interaction with a physical salesperson also offer a level of reassurance, as it is often the direct engagement with sellers that involves forceful persuasion, which deters customers in a conventional retail setting. Conversely, the buyer can contact the vendor anytime for product details. Furthermore, one can establish an understanding of the operation and quality of the desired goods or service by reaching out to the seller based on the ratings and comments provided by past buyers. When purchasing digital items like movies, music, and computer programs, if there is no requirement for a physical medium, the customer receives them instantly upon completing the purchase. Some of these conveniences are presented in Figure 2:



Figure 2. Many conveniences of online shopping for customers.

One of the drawbacks and disadvantages of the online store is the lack of transparency in the purchasing process, where customers are unaware of the exact nature of their purchase until they receive the product physically. The delivery of purchased things on the Internet can frequently be excessively long, depending on the chosen delivery provider and the merchant’s practices. In specific merchants, there is still a delay of several weeks before buyers receive the things they have ordered, even if payment is made quickly. When considering the potential necessity of replacing the item, it becomes evident that this is a meticulous and time-consuming procedure that cannot adequately replicate the shopping experience in a brick-and-mortar store. An unfavorable aspect of online stores is the growing occurrence of “discounts” on single payments, which refers to significant price differences between one-time cash payments, single installment card payments, and card payments

in multiple installments. Conventional trade often does not establish such distinctions and avoids engaging in unfair trading tactics.

3.2. The Importance of GDPR for the Growth of Online Consumption

One of the primary concerns when deciding to purchase online stores is the potential exposure of private data. Prior research has indicated that numerous customers have expressed apprehension regarding privacy when using the Internet, particularly when purchasing online. However, these worries have not aligned consistently with their actual behavior, a phenomenon known as the privacy paradox.

Marketing firms possess expertise in constructing extensive consumer datasets and thoroughly analyzing purchasing patterns. Tracking clients and visitors is effortless today, and significant insights into their behavior can be derived from user activity. None of these issues would pose a problem if the gathered data is utilized ethically. However, the combination of aggressive advertising and the sale of visitor data creates the potential for its misuse. These issues give rise to apprehensions over protecting personal data and privacy, particularly among customers. Subsequently, authorities have become concerned about mitigating potential adverse consumer effects by implementing more stringent legislative frameworks. The GDPR rule has enhanced security measures in the Member States of the European Union. Specifically, it ensures that if a user withdraws consent, their card data entered during an online transaction will not be retained in the merchant's cloud storage. There exists a certain level of friction between consumers and traders inside the realm of e-commerce. E-commerce platforms must gather personal data from current and prospective customers to facilitate transactions.

Consumers are responsible for recognizing potential risks, such as identity theft and other possible exploitation. Hence, organizations must acknowledge online consumers' preferences and requirements to establish a secure atmosphere that nurtures trust with consumers, enabling them to divulge their personal information. The premise is that regulation should reinstate customer trust in the security of online purchasing, thereby resulting in a favorable effect on the development of consumption. This paper will examine the impact of implementing more stringent legislation on personal data privacy on the expansion of online commerce and its effect on consumer behavior.

4. Digital Marketing in e-Commerce

Despite its initial appearance as a convoluted and expansive concept, digital marketing is an empowering and productive strategy. It can be defined as a collection of marketing strategies that utilize various digital technologies and media to advertise products, services, and businesses. Due to the advancement of digital services and the overall digitalization of multiple aspects of life, there is a clear and observable shift towards conducting activities online. Many mobile devices, including smartphones, tablets, PCs, and any device with an Internet connection, play a dominant role. Due to this rationale, digital media is supplanting traditional means of advertising since more corporations are choosing this method over newspaper and radio ads. This form of advertising not only has a broader reach to specific target groups, but a company can also effectively identify these target groups based on factors such as location, age, gender, and other vital parameters. This allows the company to allocate its marketing budget accurately and promote its products or services to the intended customers. Another crucial aspect is the feasibility of evaluating the campaign's efficacy, a capability that was absent in conventional advertising methods. Online advertising, known as OBA (Online Behavioral Advertising), relies on surveilling and profiling individuals' browsing habits. Web tracking entails identifying a user's browser, application, or device using identifiers like HTTP cookies. This process involves collecting user data as the user navigates across different websites. User profiling is conducted online to evaluate user behaviors based on extensive historical data gathered through tracking. This OBA technique is widely recognized as one of the most efficient means of advertising. However, users frequently express apprehension regarding potential privacy infringements.

4.1. The Importance of Digital Marketing for Online Commerce

The daily presence of more people on the Internet and the growing number of competitors selling their products and services make it crucial to stand out and reach more customers. Companies without an online store or advertising practically don't exist and don't have a growth perspective in trade, with some exceptions. Google is the top search engine that generates over 90% of Internet traffic. Thus, showing a company on search engines, either through search results or paid advertising through prominent tools, is crucial. Quality campaigns can give you an edge over the competition, no matter how strong and widespread it is. Internet visibility and presence will increase whether paid-per-click ads (PPC ads), PPM ads, or SEO optimization are discussed. Another benefit of Internet marketing is that it allows two-way communication, customer participation in offer creation, and company feedback. Many Internet marketing tools allow precise target audience definition, which is difficult in other advertising. Cost is also essential, especially for smaller companies that cannot afford expensive marketing strategies, such as Internet advertising, which is cheaper than television advertising. The adaptability of digital marketing allows companies to adjust their strategies in response to market changes, making them more competitive. Properly using digital Internet marketing tools increases Internet visibility, which increases online store traffic and revenue. These tools yield transparent and measurable results, insight into campaign quality, and the ability to adjust future strategies for better results and higher ROI (Return On Investment). In addition to advertising, digital marketing boosts the store's image, brand, growth, and customer connectivity, which increases online store revenue.

4.2. Effects of GDPR and ePrivacy on Digital Marketing

New regulations and the redefinition and tightening of some existing regulations present new challenges to the advertising industry, with digital marketing facing the most significant challenge. The GDPR is thought to have improved business data management tools.

Small advertisers and agencies face many challenges from Google, Facebook, and Apple's announcements about third-party cookie abolition. Disabling data tracking through these companies' tools and services will considerably complicate small companies and advertisers' data collection, precise target group identification, and campaign success analysis. After the user withdraws opt-out, half of marketing agencies stop web tracking, meeting user expectations. These changes will also boost marketing giants, posing many challenges to small businesses. Users may read the privacy policy, but legal and technical terminology in long, complicated texts is hard to understand. Obtaining parental consent to process child data and respecting the data subject's right to revoke consent are increased GDPR requirements.

5. Research Objectives and Methodology

Due to the pandemic and store closures, many Croatians had to buy online for the first time. Given citizens' distrust of new technologies and the provision of personal data, especially financial ones like credit card numbers, it is interesting to see if stricter regulations have created trust in this type of purchase. In addition to more stringent regulations, it is interesting to study whether the regulation affected online commerce more or caused the inability to shop traditionally.

5.1. Questionnaire and Data Collection

This study aims to examine and demonstrate the level of awareness among users regarding the vulnerability of their data on the Internet and the impact of stricter regulations on personal data protection on the trust and acceptance of online stores when users share their personal information. The questionnaire aims to examine respondents' understanding of Internet data security, their awareness of indicators of secure communication, and their views on the potential advantages of more stringent regulations for them as users.

The research and data collection was conducted using a questionnaire administered through the Google Forms platform, widely recognized as a free and commonly used tool for conducting survey

research. The data collection period spanned ten consecutive days from September 1st to September 10th, 2021. Due to the requirement of being of legal age, data analysis was limited to individuals over 18. The sample size consisted of 100 respondents. The questionnaire was disseminated via social networks and directly emailed to acquaintances.

5.2. Structure of the Data Protection Questionnaire

The questionnaire comprises 33 questions categorized into three sections. The initial section focuses on gathering demographic information from respondents, including age, gender, residence, education, and income. The second set of questions pertains to the overall understanding of computer and Internet operations, familiarity with safeguarding personal data privacy, and the ability to identify secure websites based on specific indicators. The third set of questions pertains to the respondents’ experience with an online store, including the frequency of purchases before and after implementing stricter regulations, the types of goods and services they most frequently purchase online, and their overall shopping experience.

5.3. Results Analysis

The analysis of survey data collected from a targeted demographic focuses on perceptions, behaviors, and attitudes toward personal data protection in e-commerce. As digital commerce environments evolve, so does the regulatory framework governing data security and consumer privacy. This necessitates an examination of public sentiment and the effectiveness of regulations like the GDPR.

This study aimed to evaluate the correlation between enforcing stricter data protection regulations and their perceived impact on consumer trust and behavior in online markets, with a specific emphasis on Croatia. This analysis is pivotal for determining whether consumers perceive enhanced regulatory measures as adequate protections or if they are undermined by practical challenges or a lack of awareness. Insights derived from this analysis aim to contribute to understanding the interplay between legal measures and consumer trust in digital commerce, suggesting pathways for enhancing data protection strategies in e-commerce.

5.3.1. Demographic Overview

In the study, data were collected from a total of 100 participants. The demographic distribution of the respondents, as depicted in Figure 3, reveals a gender composition where 58% were identified as male and 42% as female. Age-wise, most respondents, constituting 34%, were aged between 36 and 45. This group was closely followed by those aged 26 to 35, representing 32% of the sample. Respondents aged 18 to 25 comprised 15% of the population, whereas those between 46 and 55 accounted for 13%. The smallest age group, respondents over 56, comprised 6% of the sample.

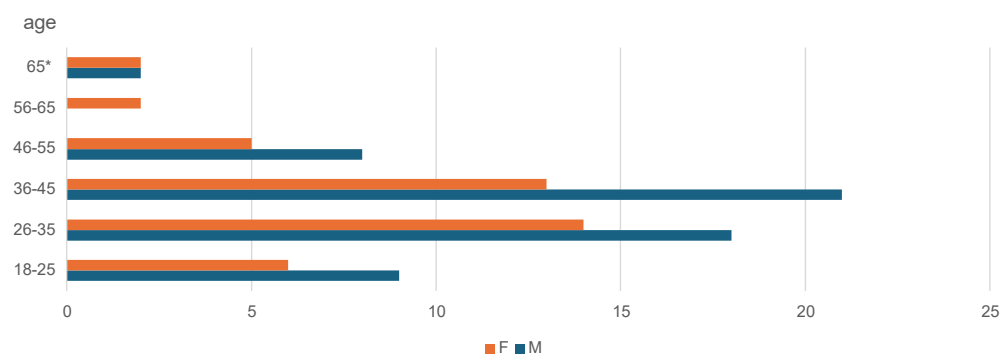


Figure 3. Structure of respondents by gender and age.

The educational qualifications of the respondents reveal that 63% of participants possess higher education, while 37% have attained primary and secondary education. Within this distribution, individuals with secondary education predominate, comprising 34% of the sample. Those with graduate studies constitute 25%. Furthermore, 19% of the respondents reported having undergraduate degrees, and 13% have completed either a postgraduate specialist study or a scientific master's degree. Respondents with postgraduate university qualifications or doctoral degrees account for 10%, and the smallest group, those with only primary education, comprises 3% of the sample.

The employment relationship data reveal that 68% of the participants are employed, 19% are students, 8% are unemployed, 3% are pensioners, and 2% have not disclosed their employment status. Regarding earnings, the highest % of respondents, 27%, report a monthly income exceeding EUR 1,500.00. Another 20% earn between EUR 1,001.00 and EUR 1,200.00 monthly, while 18% receive EUR 501.00 to EUR 1,000.00. Approximately 16% of the participants have no income, and 6% earn up to EUR 500.00 monthly.

Regarding residence, 37% of the respondents live in areas with populations exceeding 150,000. Smaller communities with 10,001 to 50,000 inhabitants house 23% of the respondents; 16% reside in areas with 100,001 to 150,000 inhabitants, 14% in communities with fewer than 10,000 people, and 10% in regions housing 50,001 to 100,000 inhabitants. For household composition, the largest group, 27%, consists of households with four members, followed by three-member households at 21%, two-member households at 20%, and individuals living alone at 18%. Households with five members account for 10%, those with six members comprise 3%, and the smallest group, 1%, has nine members.

Concerning marital status, the most significant % of respondents, 43%, are single. Married respondents comprise 38% of the sample, 15% live with a partner, and 4% are widowed.

Data on household composition indicate that the most significant proportion of respondents, 27%, reside in households consisting of four individuals. Households with three members account for 21% of the sample, followed closely by two-person households comprising 20%. Eighteen percent of participants live alone. Ten percent of the respondents are part of five-member households, while households with six and nine members represent 3% and 1% of the sample, respectively.

The second segment of the questionnaire aimed to evaluate respondents' perceptions of their competencies in computer operation, Internet usage, and personal data privacy protection, including their ability to recognize indicators of secure websites. Respondents were asked to rate their skills using a Likert scale from 0 (representing computer illiteracy) to 7 (indicating expert computer skills). The analysis reveals that respondents generally perceive their IT literacy as high, with the average score across attributes being 5.25 and the most frequent response being 6. Notably, individuals aged between 36 and 45 reported higher levels of IT proficiency, whereas those aged 56 to 65 tended to rate their computer knowledge lower.

Respondents were queried about the frequency of their Internet use. The results show that a significant portion of the participants are frequently online: 37% reported always being connected, 28% very often, 24% relatively often, 9% sometimes, and a small minority of 2% rarely use the Internet. This indicates a high level of Internet presence among the respondents.

5.3.2. Data Security and Privacy Awareness

Additionally, the survey explored respondents' understanding of personal data protection. This included assessing their knowledge of what constitutes personal data, aiming to gauge their awareness and comprehension of data privacy issues.

An analysis of survey responses revealed exciting insights into what respondents consider personal data. As shown in Table 1, a significant misconception was observed; 66% of respondents incorrectly identified the registration number of a legal entity as personal data, and 58% made the same error with the financial data of legal entities. Additionally, it is particularly noteworthy that 40% of respondents do not recognize students' school grades as personal data. These findings highlight gaps in understanding what constitutes personal data among the public.

Table 1. Personal data perception.

Personal data	Yes
First and last name	86%
Physical address	89%
E-mail address	72%
Citizen identification number	91%
Company identification number	66%
Bank account	63%
IP address	78%
Company financial data	58%
Student grades	60%
Personal ID number	87%

The research reveals significant concerns among respondents regarding their online data security. The majority, 58%, identify the unauthorized sharing of their data as the primary threat. Cybercriminals are considered a potential threat by 49% of the respondents, followed by the threat of employee data theft at 40%. Accidental data loss is noted by 34%, while 29% are concerned about misuse of personal data by another country, and 25% by data breaches related to terrorist activities.

Regarding computer protection, 78% of respondents report installing antivirus systems on their PCs, highlighting a prevalent adherence to basic cybersecurity measures. Despite this, only 26% of respondents feel secure about their data online, with a scant 7% feeling extremely secure, indicating widespread unease about online data safety.

A substantial 74% of participants strongly agree on the importance of Internet security, with an additional 16% generally agreeing. Only a tiny fraction (5%) disagree, and 2% view online security as unimportant. When asked about experiences with online fraud, 64% have not encountered fraud, whereas 37% have faced some inconveniences while shopping online.

Negative online shopping experiences have led to significant behavioral changes among consumers. Of those affected by such experiences, 14% temporarily ceased online purchases, and 7% stopped altogether. Conversely, 52% now purchase only from verified retailers post-experience, demonstrating a cautious approach to online shopping, while 28% report no change in their shopping behavior.

According to guidelines from the European Commission, safe online purchasing practices include verifying that a website uses the “https://” protocol and displays a locked padlock icon, indicating secure data transmission. Websites labeled with “http://” or displaying an unlocked red padlock or exclamation mark are deemed insecure for transmitting personal information.

Survey results show that a significant % of respondents, 63%, adhere to these security guidelines when shopping online. However, 39% of the participants do not consistently observe these safety measures during online transactions. This indicates a gap between awareness and practical security measures among Internet users.

Regarding cookie consent, 40% of respondents admit never reading the terms of use for cookies before consenting. Meanwhile, 42% have read these terms at least once but do not revisit the documents, simply accepting the cookies subsequently. A more cautious 20% always review the cookie terms each time they visit a new site.

When it comes to types of cookies, technical cookies, which are essential for website functionality and cannot be disabled, received consent from 54% of respondents; functional cookies, which can be turned off and used to enhance site functionality and personalization, are accepted by 20% of respondents. Marketing cookies, used for tracking and delivering targeted advertising, are consented to by 12%, and statistical cookies, which track site activity and effectiveness, are accepted by only 9% of respondents. Surprisingly, 36% of respondents indicated they consent to all types of cookies presented.

5.3.3. Consumer Trust and Regulatory Impact

The third set of questions in the survey addressed the respondents’ online shopping experiences, including the frequency of purchases before and after the enactment of stricter data protection regulations, the types of goods and services commonly purchased online, and general shopping experiences. The majority of respondents, 38%, reported shopping online every month. Annually, 29% of respondents make purchases, and 19% shop weekly. An equal percentage of 7% either shop daily or do not shop online.

Respondents’ familiarity with the GDPR varied, with 57% indicating partial familiarity. Twenty-two percent of respondents reported complete familiarity with the regulation, while 21% were unfamiliar.

The GDPR’s impact on respondents’ confidence in online shopping was significant, particularly among those aged 36-45, who reported the highest influence, rating their increased trust with the highest score of 7 on a Likert scale. In contrast, the youngest and oldest age groups reported no significant change in trust levels, whereas middle-aged groups showed increased confidence in online shopping.

Familiarity with the GDPR across different age groups showed that 94.12% of respondents aged 36-45 years were fully or somewhat familiar with the regulations, with only 5.88% lacking any familiarity. This pattern of familiarity was generally higher among respondents with higher educational backgrounds, with 96% of those holding a graduate or undergraduate degree reporting some level of understanding.

As shown in Figure 4, regarding the frequency of online purchases post-regulation, 26% of respondents who previously shopped infrequently (“rarely”) perceived an increase in their shopping frequency, suggesting a minimal but noticeable shift toward more frequent online shopping following stricter regulations. However, no significant increase was observed in other respondent groups regarding shopping frequency post-regulation.

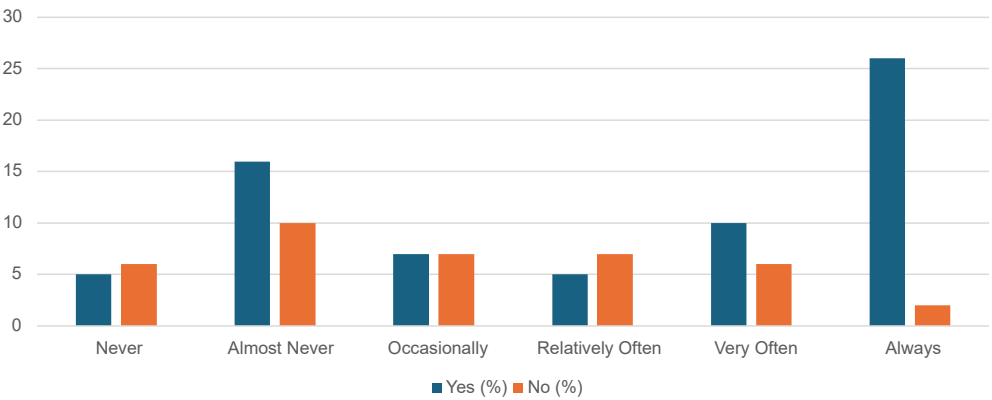


Figure 4. Frequency of online purchases.

They dominated product categories purchased online: clothing, footwear, and fashion accessories, with 59% of the sample purchasing them. Information technology, home appliances, and sports equipment were popular categories, with 41% and 37% of respondents purchasing these items.

Survey results, as shown in Figure 5, indicate significant concerns among respondents regarding online shopping, with the highest anxiety centered around credit card misuse (59%), followed by fear of fraud (48%) and personal data theft (47%). 42% of respondents reported concerns about losing money, and the inability to return purchases concerned 28%. Additional worries included the cost and potential taxes on shipping (24%), while 16% expressed a general distrust of online shopping. Only 1% were concerned about not receiving their ordered items.

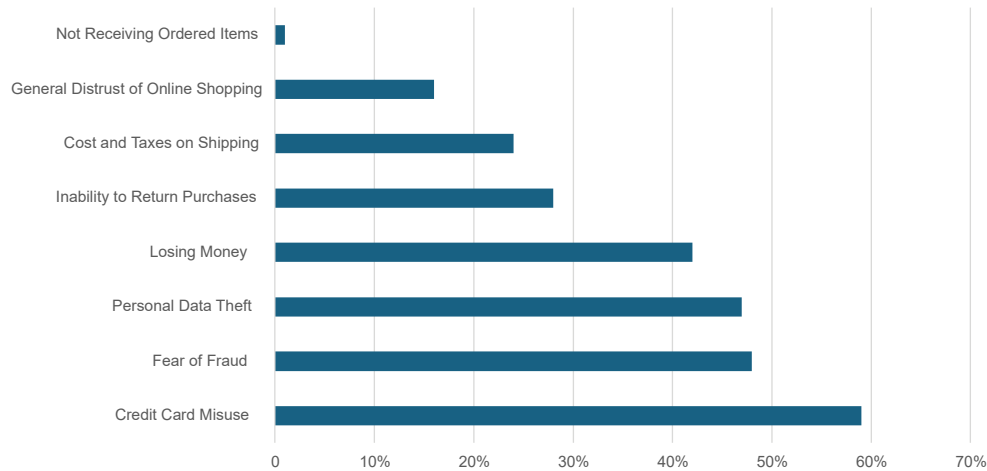


Figure 5. Concerns regarding online shopping.

5.3.4. Payment Methods and Economic Trust

When queried about preferred online payment methods, cash on delivery was the most popular, chosen by 50% of respondents, indicating a lack of trust in online transactions and fear of fraud and card misuse. PayPal was the preferred option for 35%, while 25% opted for debit card payments. A lesser-used method was credit card payments (24%); only a tiny fraction (6%) used Google Checkout. 2% of respondents indicated they do not make payments online, presumably in scenarios where online stores do not offer cash on delivery.

5.3.5. Factors Influencing Online Retail Choices

The quality of products was the most critical factor for 57% of respondents when choosing an online retailer. Customer reviews significantly influenced 52% of respondents, and competitive pricing was important for 47%. Other factors included ease and conditions of returns (30%) and product availability (28%). Product descriptions (27%), assortment breadth (24%), and content clarity (20%) were also notable factors.

Most respondents (55%) prefer shopping from foreign online retailers due to better pricing. Foreign platforms like Aliexpress, Amazon, and eBay typically offer more competitive rates than domestic markets.

5.3.6. Ad Blocking and Personalized Advertising

Regarding ad blocking, 54% of respondents denied using any ad-blocking software, while 47% confirmed its use. This suggests a division in how respondents manage their online privacy and advertising exposure.

5.3.7. Attitudes towards Data Brokers and Privacy

The survey also explored respondents’ awareness of targeted advertising, with a significant number confirming their understanding (61%), while 39% were unfamiliar with the concept. This awareness might influence the acceptance of personalized advertising among those not using ad-blocking technologies.

Lastly, when asked about their views on data brokers collecting data to create detailed consumer profiles for targeted advertising, 59% of respondents viewed this as a significant issue, 22% as a moderate problem, 15% as a minor problem, 1% as a minor problem, and only 3% saw no issue with these practices.

6. Discussion

The examination of survey data reveals an intricate picture of consumer behavior and trust dynamics in the digital commerce environment. The survey found that although a large section of the public has high IT literacy and uses the Internet frequently, there is still a considerable difference between how people view their ability to secure their data and their understanding of personal data. The presence of misunderstandings regarding the nature of personal data, such as the improper categorization of legal entity data as personal information, highlights the necessity for improved educational initiatives in conjunction with regulatory actions.

6.1. The Effectiveness of GDPR and Its Broader Consequences

The enactment of the GDPR has been a fundamental aspect of recent endeavors to strengthen online privacy and data security. The implementation of this legislation seems to have had a significant impact on consumer attitudes, especially among middle-aged consumers who exhibited the most essential levels of familiarity and confidence. Nevertheless, the many perspectives on GDPR, which span from strict compliance to noticeable deficiencies in adherence, indicate that the implementation of legislation is inadequate without vigorous enforcement and extensive public education initiatives.

Although a robust legal structure exists, our research reveals that 39% of consumers do not consistently adhere to the suggested security protocols while making online purchases, such as ensuring secure connections and website validity. This discrepancy is undoubtedly a contributing factor to the ongoing worries about the misuse of credit cards, fraudulent activities, and data theft.

6.2. Impact of Socio-Economic Factors on Online Behavior

Age, education level, and socio-economic position are important demographic parameters that considerably impact online behavior and how people perceive security. Younger and more educated individuals show higher levels of adaptation and reactivity to changes in data protection legislation, possibly because of their better digital literacy rates. In contrast, the older and less educated portions of the population exhibit decreased levels of trust and adherence to security practices, indicating the existence of a digital gap that regulatory authorities and e-commerce platforms need to tackle.

The economic ramifications are also apparent in the payment methods favored by consumers. The high frequency of cash on delivery, viewed as a more secure technique, suggests a persistent lack of faith in online payment systems. Robust security measures and clear consumer protection regulations are crucial for instilling trust in electronic payment systems.

6.3. Guidelines for Strengthening Data Protection Strategies

To address the disparity between consumer confidence and the efficacy of data security tactics, several solutions are suggested:

- **Enhanced Education and Awareness Campaigns:** Focused educational initiatives that elucidate the definition of personal data and provide guidance on safeguarding it can effectively mitigate misunderstandings and improve consumer proficiency;
- **Enhancing Regulatory Enforcement:** Implementing stricter enforcement measures for current legislation and periodic audits of e-commerce platforms will guarantee improved compliance and foster confidence;
- **Improved Transparency and Communication:** Businesses should enhance their level of transparency about the utilization of consumer data and ensure that privacy policies and terms of service are presented more explicitly and easily;
- **Adoption of Advanced Security Measures:** E-commerce platforms must adopt modern security measures, such as encryption and two-factor authentication, to ensure the adequate protection of consumer data.

These guidelines can significantly improve consumer confidence and data security effectiveness. Businesses can make e-commerce safer by prioritizing education, regulatory enforcement,

transparency, and advanced security. These efforts will protect consumer data and build user trust and loyalty.

7. Future Work

Various areas for additional research are suggested to tackle the changing difficulties and possibilities in data protection. By delving into sophisticated privacy-enhancing technologies (PETs), it is possible to provide more robust safeguards for consumer data while maintaining functionality. This can establish a standard for future security measures in digital commerce settings. Performing longitudinal research to evaluate the progression of consumer behaviors about online shopping and data sharing about shifting privacy rules and technologies will yield significant observations on consumer trust fluctuation over time.

It would be advantageous to compare data protection laws and their efficacy in various cultural and regulatory contexts, particularly between EU nations subject to GDPR and those not under its jurisdiction. These studies would emphasize the worldwide influence of data protection standards and assist multinational e-commerce platforms in customizing their privacy policies more efficiently.

Measuring the explicit and implicit expenses of data breaches on e-commerce enterprises, which include effects on consumer confidence and customer loyalty, should emphasize the economic significance of investing in thorough cybersecurity measures. Examining the consequences of developing technologies like artificial intelligence and blockchain on the security of personal data in e-commerce is crucial, as these technologies are significantly changing the e-commerce industry.

Given the swift advancement of technology and changes in consumer behavior, it is crucial to examine and maybe revise current regulatory frameworks that oversee data protection. Creating and evaluating real-time monitoring and response systems for data breaches could significantly reduce the harm caused by these events, hence increasing consumer trust. These projects aim to enhance e-commerce data protection by improving our understanding of technological, behavioral, and regulatory aspects. They ensure that strategies address existing deficiencies and anticipate future difficulties in the digital commerce sector.

8. Conclusions

This study thoroughly investigates the relationship between more stringent data protection legislation and its perceived effects on consumer trust and shopping behaviors in Croatia's e-commerce industry. The study employed an extensive survey to gather consumer opinions and actions, offering a thorough demographic overview and insights into understanding personal data security.

Our research indicates that although most people have a substantial degree of Internet usage and knowledge of information technology, there are still notable deficiencies in their comprehension and implementation of measures to safeguard personal data. Significantly, many participants demonstrated misunderstandings regarding the definition of personal data, highlighting the necessity for improved educational initiatives to address these gaps.

The implementation of the GDPR has significantly influenced how middle-aged Internet users, who are most knowledgeable about the rule, perceive and trust online platforms. However, the survey found that a substantial portion of the population does not consistently follow suggested Internet security practices, which might undermine the effectiveness of regulatory efforts.

From an economic standpoint, the research emphasized a careful attitude towards online transactions, as indicated by a widespread inclination to choose cash on delivery. This preference arises from a persistent lack of trust in digital payment systems. This highlights the essential requirement for e-commerce platforms to strengthen their security measures to enhance consumer trust and promote more secure online purchasing participation.

As we consider the future, regulatory agencies and e-commerce enterprises must maintain their collaboration to advance a more secure online buying environment. This entails complying with rigorous data privacy regulations and actively participating in consumer education to guarantee that

individuals are adequately educated about their rights and the safeguards implemented to safeguard their personal information.

In conclusion, although the more stringent legislation have established a structure for enhanced security and confidence, the main obstacle is guaranteeing their successful execution and continuously educating the consumer population to achieve a genuinely secure and reliable e-commerce environment in Croatia.

Author Contributions: Conceptualization, Z.M. and D.D.; Methodology, Z.M. and D.D.; Validation, V.D. and D.R.; Formal analysis, D.D. and D.R.; Investigation, Z.M. and V.D.; Resources, Z.M.; Writing—original draft, Z.M. and D.D.; Writing—review & editing, V.D. and D.R.; Supervision, V.D.; Project administration, Z.M. and V.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Arora, D. Data Privacy Issues with E-Commerce. *Int. J. Soc. Sci. Econ. Res.* 2023, 8, 1167–1174. <https://doi.org/10.46609/IJSSER.2023.v08i05.020>.
2. Muneer, A.; Razzaq, S.; Farooq, Z. Data Privacy Issues and Possible Solutions in E-commerce. *J. Account. Mark.* 2018, 7, 294. <https://doi.org/10.4172/2168-9601.1000294>.
3. Boritz, J.E.; No, W.G.; Sundarraj, R.P. Internet Privacy in E-Commerce: Framework, Review, and Opportunities for Future Research. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) 2008*. <https://doi.org/10.1109/HICSS.2008.215>.
4. Ghani, N.A.; Sidek, Z.M. Personal information privacy protection in e-commerce. *ACM DL Digital Library, WSES Transactions on Information Science and Applications*, Vol.6, No.3. Available online: <https://dl.acm.org/doi/10.5555/1553642.1553649> (accessed on 17 July 2024).
5. Salim, S.C.; Neltje, J. Analysis of Legal Protection Towards Personal Data in E-Commerce. *Proceedings of the 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021) 2022*. <https://doi.org/10.2991/assehr.k.220404.101>.
6. Moores, T.T.; Dhillon, G. Do Privacy Seals in E-Commerce Work? *Commun. ACM* 2003, 46, 265–271. <https://doi.org/10.1145/953460.953510>.
7. Zhong, G.; Wang, Z. Consumer Privacy Protection of E-Commerce. *Proceedings of the 2018 International Symposium on Social Science and Management Innovation (SSMI 2018) 2019*. <https://doi.org/10.2991/ssmi-18.2019.35>.
8. Farah, B.N.; Higby, M.A. E-Commerce and Privacy: Conflict and Opportunity. *Journal of Education for Business* 2001, 76, 303–307. <https://doi.org/10.1080/08832320109599653>.
9. Antoniou, G.; Batten, L. E-Commerce: Protecting Purchaser Privacy to Enforce Trust. *Electron Commer Res* 2011, 11, 421–456. <https://doi.org/10.1007/s10660-011-9083-3>.
10. Bella, G.; Giustolisi, R.; Riccobene, S. Enforcing Privacy in E-Commerce by Balancing Anonymity and Trust. *Computers & Security* 2011, 30, 705–718. <https://doi.org/10.1016/j.cose.2011.08.005>.
11. Budiono, A.; Shaharani, Z.; Prakoso, A.L. Consumer Legal Protection Against Default in Buying and Selling E-Commerce. *jurnaljustisi* 2023, 9, 93–103. <https://doi.org/10.33506/jurnaljustisi.v9i2.2317>.
12. Gadjong, A.A. The Agreement of Personal Shopping Service through E-Commerce Platforms: A Case Study of Consumer Protection. *sjh* 2023, 4, 388–401. <https://doi.org/10.37276/sjh.v4i2.230>.
13. Lu, R. Computer E-Commerce Security System Under the Background of Big Data. 2020 International Conference on Robots & Intelligent System (ICRIS) 2020. <https://doi.org/10.1109/ICRIS52159.2020.00106>.
14. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Applied Sciences* 2023, 13, 1020. <https://doi.org/10.3390/app13021020>.
15. Monsalve-Obreque, P.; Vargas-Villarreal, P.; Hormazabal-Astorga, Y.; Hochstetter-Diez, J.; Bustos-Gómez, J.; Diéguez-Rebolledo, M. Proposal to Improve the E-Commerce Platform Development Process with an Exploratory Case Study in Chile. *Applied Sciences* 2023, 13, 8362. <https://doi.org/10.3390/app13148362>.
16. Duarte, C.; Messias, I.; Oliveira, A. Technological Acceptance of E-Commerce by Generation Z in Portugal. *Information* 2024, 15, 383. <https://doi.org/10.3390/info15070383>.
17. Chen, Y.; Feng, L.; Zhao, Q.; Tian, L.; Yang, L. ARS-Chain: A Blockchain-Based Anonymous Reputation-Sharing Framework for E-Commerce Platforms. *Mathematics* 2024, 12, 1480. <https://doi.org/10.3390/math12101480>.

18. Burlacoiu, C. Online Commerce Pattern in European Union Countries between 2019 and 2020. *Societies* 2022, 13, 4. <https://doi.org/10.3390/soc13010004>.
19. Kim, S.S. Purchase Intention in the Online Open Market: Do Concerns for E-Commerce Really Matter? *Sustainability* 2020, 12, 773. <https://doi.org/10.3390/su12030773>.
20. Marjerison, R.K.; Zhang, Y.; Zheng, H. AI in E-Commerce: Application of the Use and Gratification Model to The Acceptance of Chatbots. *Sustainability* 2022, 14, 14270. <https://doi.org/10.3390/su142114270>.
21. European Ecommerce Report 2019 edition, Ecommerce Europe. Available online: https://www.ecommerce-europe.eu/wp-content/uploads/2019/07/European_Ecommerce_report_2019_freeFinal-version.pdf (accessed on 18 July 2024)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.