Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 219 (2023) 767–777

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022

Exploring the Impact of GDPR on Big Data Analytics Operations in the E-Commerce Industry

Moutaz Haddara[a], Salazar, A[b], Marius Langseth[a,*]

[a]*Kristiania University College, 0107 Oslo, Norway.*
[b]*TIAS School for Business & Society, 3511 RC Utrecht, Netherlands.*

Abstract

This research explores the impact of data privacy and protection laws on e-commerce companies in the Netherlands. Specifically, this study focuses on the General Data Protection Regulation (GDPR). The purpose of this regulation is to refine privacy laws and emphasize the importance of consumer protection and consent. GDPR might challenge enterprises, especially data-driven organizations. Notably, the e-commerce industry is known for relying heavily on big data analytics, business intelligence, and other data-related technologies. Multiple semi-structured interviews with e-commerce professionals and consumers were conducted to gain a deeper understanding of the impact of GDPR based on the strategies employed by e-commerce companies and the online user experience of customers in the Netherlands. The main findings show that while GDPR compliance incurred additional costs for companies, it also improved data security and increased customer trust. Furthermore, the results also suggest that GDPR affects the e-commerce analytics operations in organizations after its adoption. Thus, many organizations have altered their practices to achieve compliance with the laws. The findings of this research contribute to the ongoing exploration of the effects of GDPR on online retail businesses that utilize (big) data analytics.

Keywords: GDPR; Data Privacy Law; E-commerce; Big Data; Data Analytics.

* Corresponding author. Tel.: +47 977 15 767.
E-mail address: marius.langseth@kristiania.no

10.1016/j.procs.2023.01.350

1. Introduction

Online shopping has become an increasing trend as more people find it easier to purchase goods and services through the internet. The e-commerce industry continues to expand as online sales worldwide are expected to grow as high as 21.8% in 2024 [1]. In the Netherlands, the annual online revenue is estimated at 26.6 billion euros in 2020, with over 80% of the population shopping online [2]. While it is convenient for consumers to buy everything online, they are required to provide 'sensitive' and private personal information to proceed with their online transactions. This personal information may include the customer's name, address, contact details, bank account details, likes, clicks, reviews, etc. Most companies use this information to recommend related products, upgrade customer service, advertise, and devise other marketing techniques and strategies. These are all made possible thanks to Big Data Analytics (BDA). BDA plays a vital role in extracting large datasets and identifying patterns from current and historical data to gain valuable insights relevant to effective decision-making. Nowadays, e-commerce companies use predictive algorithms heavily for their recommendation systems to personalize customers' shopping experience [3]. Data analytics also analyze consumer patterns and behaviors, forecast products, and distribute demand [4]. On the other hand, the rapid change in technology entails that when more data is collected and stored on the internet, information privacy and security risks-related issues multiply. Previous data regulations have not included guidelines to resolve many of those issues. For that reason, the General Data Protection Regulation (GDPR) was established in 2016 and enforced on May 25, 2018. GDPR has provided clear sets of regulations that aim to protect and govern the fundamental privacy rights of people, update privacy laws, and amalgamate the 28 distinct privacy laws of the EU member states [5]. The GDPR is still an ongoing challenging issue, as some companies struggle to make a series of adjustments in their operations. Implementing these methods and regulations in information systems' infrastructures requires extra effort during the design phase, which will most likely influence the system's performance [6]. Additionally, Xuereb, et al. [7] argue that firms would have to allocate a higher budget for employee resources, new training programs, and other related costs to adhere to this new law. Aridor, et al. [8] also examined the potential economic implications of GDPR as consumer behavior changes after the increase in consent requirements. The e-commerce industry suffered a significant decrease of 13% in sales and 12% in recorded page views following the GDPR activation [9]. These studies establish how GDPR negatively affects businesses. Some companies, however, affirm that no extensive changes occurred in their operations [10], and other studies even indicate a positive outlook from the customers' perspective [11, 12]. Four years into effect, no conclusive findings have been found on the impact of GDPR on the economy. On top of that, previous research's attempts to measure the impact of GDPR on firms' performance have focused solely on examining the companies' online revenue, profit margins, and operating expenses pre-and-post-GDPR. Further, little is known about the mechanisms through which GDPR can influence e-commerce firm operations by looking at the companies' systems, analytics, and algorithms. To bridge this literature gap, investigating the limitations set by GDPR in BDA will be a crucial topic for e-commerce companies in the Netherlands and other countries within the European Union.

Based on the previous discussion, the main research question for this paper is: To what extent does the General Data Protection Regulation (GDPR) influence e-commerce analytics in the Netherlands? The following sub-questions were formulated to answer the main research question: What is GDPR, and what are its scope and limitations? What are the problems e-commerce companies encounter in GDPR implementation? What changes have been made in e-commerce analytics tools, strategies, and techniques following the GDPR implementation? The remainder of the paper is organized as follows. A review of GDPR and analytics are provided in section 2. Section 3 explains the methodology utilized in this research. Section 4 presents the findings, and finally, a conclusion is provided in section 5.

2. Related Research

GDPR is characterized as a data protection legislation that sets the rules for organizations on how to process, store, analyze, and manage data from people residing within the European Union area [13]. As more companies rely heavily on data for their business processes and routine operations, GDPR was adopted by the European Parliament to oblige companies to inform and explain explicitly to their customers their data collection process and how their data will be used, secured, analyzed, and shared. Before GDPR, the 1995 Data Protection Directive (DPD) was used to protect people's right to privacy. However, the primary concern with DPD is that it does not include provisions concerning

the use of modern technology. Aside from that, several policies and regulations have been observed by different countries in the European Union before GDPR's implementation. GDPR's enforcement serves to unify and empower data protection regulations within the EU Moreover, GDPR has refined previous European privacy regulations and highlighted the importance of consumer consent and privacy rights. New rules indicated how consent should be "freely given, specific, informed and unambiguous" [13]. While GDPR has many articles (99) covering various aspects, this paper focuses solely on articles that deem relevant to or may influence BDA operations.

2.1. Overview of related GDPR Articles

In the regulations, Article 2 discusses the material scope of GDPR, while Article 3 of GDPR sheds light on the territorial content of the law [13]. Based on this, GDPR applies to any company or organization that processes personal data as part of the activities of one of its subsidiaries based in the EU, regardless of where this data is processed. GDPR is also to be followed by companies established outside the EU which provide goods or services or track the behavior of people residing in the EU. GDPR also stipulates privacy by design and default. Data Protection by Design urges companies to consider data protection during the initial design phase and throughout the development process of any product, process, or service that requires the processing of personal data. On the other hand, Data Protection by Default means that when a system or service includes different options on how much personal information the individual can share with the company, the default settings should be set in the most privacy-friendly one. Article 25 of the GDPR further elaborates on data protection by design and default [13]. Articles 24 to 43 of GDPR lay out the responsibilities of Data Controllers and Data Processors [13].

Data Controllers and Processors could be individuals, private companies, or other legal entities. What distinguishes the two is the level of GDPR compliance responsibilities. The Data Controller's primary task is to determine how and why personal data will be processed. They have the overall authority and the key decision-makers over personal data and are expected to observe the strictest levels of GDPR compliance. This is compared to the GDPR compliance responsibilities of the Data Processors. Data Processors only operate on behalf of and with the authorization of the Data Controller in charge. Article 29 affirms that a Data Processor must only process personal data on the orders of the Data Controller unless otherwise required by law. Data Processors must take adequate measures to guarantee that data processing aligns with the GDPR. Articles 5 to 11 of GDPR outline seven protection and accountability principles relating to personal data [13]. The seven principles listed below explain how data must be gathered, processed, and stored; (1) Lawfulness; (2) Fairness and transparency; (3) Purpose limitation; (4) Data minimization; (5) Accuracy; (6) Storage limitation; (7) Integrity and confidentiality. Privacy rights aim to give individuals control over the personal information provided to businesses and other enterprises. Articles 12 to 23 stipulate these rights and assure data subjects that companies cannot use their data for anything other than the originally agreed upon [13]. The following summarizes the privacy rights of data subjects: The right to be informed; The right of access by the data subject; The right to rectification; The right to erasure; The right to restrict processing; The right to data portability; The right to object; Rights to automated decision-making and profiling. GDPR has modified the previous laws and expounded these rights to keep up with rapid technological changes. Now, individuals can request to delete their data, restrict the processing of their data, file a complaint directly to the supervisory authorities, and even reject automated processing and profiling. The new regulation also included fines and penalties for violators to ensure proper compliance with GDPR. Under Article 83, GDPR fines are specified in complete detail [13]. Accordingly, the amount of financial penalty will depend on several factors leading up to the infringement. These infringements refer to GDPR principles concerning the basic principles for data processing, conditions for consent, data subjects' rights, and data transfer to an international organization or a recipient in a third country. Besides that, individuals and employees may also be held accountable and, in extreme cases, may lead to criminal charges.

2.2. E-commerce Analytics

Based on extant literature, e-commerce analytics is defined as any business and technical undertakings to systematically analyze data in order to improve the business outcomes of organizations that sell online [14]. These include statistical analysis, data mining, predictive techniques, etc. BDA is the modern version of the traditional data mining process since it deals with the five V's of big data: volume, veracity, velocity, variety, and value, and relies

heavily on predictive analytics and data science approaches [15]. Companies adopt BDA mainly to improve their processes and gain a competitive advantage. In particular, the e-commerce industry is known for its rampant use of BDA, provided its affinity for technology. Thus, the term e-commerce analytics emerged to refer to the role of BDA in e-commerce. In simple terms, e-commerce analytics is characterized by incorporating BDA techniques into the business operations of e-commerce companies. There is a vast number of studies exploring the evolution of e-commerce analytics. Extensive research has been conducted to define the role of BDA in e-commerce. For example, Akter and Wamba [16] put these all together. They concluded that there are five aspects of BDA to consider in e-commerce: (1) customer needs identification, (2) market segmentation, (3) decision-making and performance improvement, (4) new product/market/ business model innovations, and (5) creating infrastructure and transparency. The following section will discuss the three widely used techniques of BDA in e-commerce. Namely, personalization and recommendation systems, dynamic pricing, and security and fraud detection. Personalization and Recommendation Systems- the e-commerce industry is expected to grow further in the upcoming years, and the more it expands, the more data is collected from the internet. With this dilemma, a Recommendation System (RS) is an e-commerce tool that solves the information overload issue while personalizing the user's overall experience by delivering accurate and personalized recommendations according to their preferences or online behavior [17]. In addition, RS continues to evolve into various methods and models. For example, Collaborative Filtering, which emerged in the early '90s, is a technique used to personalize users' experiences through recommendations tailored to the users' interests, leveraging the earlier experiences of other users with similar or matching profiles [18]. For over two decades, this method has been one of the contributing factors to the success of e-commerce's leading brand Amazon. Amazon's item-based CF at the user's past orders before featuring related products based on this information. Aside from CF, content-based and knowledge-based RS are also frequently used. Hence, the recommendation system is one of the powerful tools utilized to increase customer satisfaction, and for these recommendation systems to function accurately, predictive analytics are heavily incorporated. Predictive Analytics is the use of historical data to be able to predict future trends [15]. For instance, predicting which type of shirt will be the trend among teenagers in summer can provide valuable insights into the manufacturing processes of clothing brands. Because of this, online retailers better understand customers' purchasing decisions and can make informed decisions to remodel their processes and strategies. Dynamic Pricing- the E-commerce industry is highly competitive. Customers can shift from one seller to another because they can easily compare prices on the internet. To secure their market share, top online sellers often use Dynamic Pricing. Dynamic pricing can be defined as the buying and selling of products in markets where (personalized) prices fluctuate and are free to adjust in response to supply and demand conditions [19]. Dynamic pricing aims at adjusting the product's price at the right time to provide the most fitting service to a specific customer at a precise time. BDA reduces the demand uncertainty as companies take advantage of market information to analyze consumer and competitor trends [20]. Airline companies often use this strategy. Air France-KLM, for example, studies real-time sales data so they can precisely set its ticket prices according to the updated demand distribution [21]. This pricing strategy has been beneficial for revenue management and competitive positioning. Security and Fraud Detection- as more financial transactions are processed on e-commerce websites and mobile applications, the likelihood of potential fraud also increases. Fraud has been a big problem for e-commerce companies since sensitive information, such as bank account and credit card details, has been constantly targeted by scammers and fraudsters. On that note, BDA has been proven successful in identifying fraud in real-time, thus minimizing the risks for customers and e-commerce vendors. Tools and infrastructures, such as Hadoop allow e-commerce companies to analyze data at an aggregated level to detect credit card fraud and identity theft [16]. Similarly, Jhangiani, et al. [22] proposed a model using machine learning algorithms, such as Random Forest, Gradient Boost, and Adaboost, to better predict fraudulent transactions.

2.3. GDPR's Influence on Big Data Analytics and E-commerce

BDA enables companies to use large and complex data to optimize business operations and solutions. In contrast, GDPR limits the gathering and processing of personal data. For that reason, GDPR signifies challenging implications in business operations, especially for data-driven companies. Some previous studies demonstrated conflicting views on the impact of GDPR on organizations. One of which is by Engan [23], which studied the influence of GDPR on the value of data and focused on the benefits of incorporating BDA into business processes. Looking into a case study

on smart meter data, the author concluded that GDPR impedes companies' ability to drive value from big data and realize the full potential of algorithmic decision-making. However, the research also suggested that even if GDPR has a negative effect in the short-term, the new regulation strengthens customer trust and creates value in the long run. Another study by Gruschka, et al. [6], scrutinized how data processing systems have altered since GDPR implementation. They examined two real-life research projects in which privacy-preserving techniques are applied. The authors revealed two different outcomes in these two case studies: the first project found no issues in data processing, while the second one faced some setbacks since anonymization is now required.

Similarly, a few related studies provided helpful suggestions to reduce the burden of enforcing the regulation. Ajibade [24] used a doctrinal research method to investigate the relationship between GDPR and BDA. The findings indicated that GDPR's seven principles would cause several issues for any data-driven company [24]. The paper recommends creating a BDA process to improve anonymization and pseudonymization when processing a high volume of data [24]. This process could be an effective strategy to maintain the balance in using BDA while ensuring GDPR compliance. Besides that, Rhahla, et al. [25] examined GDPR by analyzing its principles, guidelines, and challenges it brings to Big Data systems. They also proposed an IT GDPR framework that aims to incorporate GDPR components into IT requirements. In addition, some research determined the early effects of GDPR on the e-commerce industry in several European countries through data analysis. For example, by examining the influence of GDPR on online user behavior before and after the GDPR enforcement, Schmitt, et al. [26] studied over 6,000 websites in various industries. Using a difference-in-difference analysis, it provided well-founded results that suggest a significant decrease in the total number of visits to websites and fewer unique visitors. Similarly, Goldberg, et al. [9] analyzed the impact of GDPR on over 1,000 websites in four months. The paper centered on the privacy regulation's effect on user website page views and website revenue. Both research papers concluded a significant decrease in revenue for e-commerce websites. These previous works denote that GDPR causes difficulties in organizations' data processing and e-commerce analytics systems. Companies are now forced to prioritize compliance with the new regulation, thus restricting the usage of BDA in their operations. As a result, current processes are foreseen to be not as effective in attracting customers and generating more revenues.

3. Methodology

The research approach adopted for this paper is qualitative research [1]. This approach is instrumental in identifying deeper issues from the perspectives of the research participants (informants) and gaining a deeper understanding of the meaning and interpretation the informants give to specific events or behaviors. Moreover, [1] noted that adopting this approach is necessary for providing flexibility and diverse viewpoints from the participants, thus leading to new and meaningful insights. With the scarcity of qualitative studies investigating the effects of GDPR on the e-commerce industry, a qualitative research approach was then chosen and applied in this study. According to [2], qualitative research is the right approach to represent the views and perspectives of the research respondents. The research design was also selected to aid in diving deeper into the issues relating to GDPR and its implications in applying BDA in the e-commerce industry. The aim is to learn about the difficulties e-commerce companies experience complying with GDPR and the consequent effects on their BDA operations.

3.1. Data Collection

For data collection, semi-structured interviews were conducted with selected professionals working in e-commerce firms operating in the Netherlands, and interviews with customers who have experience purchasing goods and services online in the Netherlands. Semi-structured interviews were chosen for this research to look at the impact of GDPR from both the company's and customer's perspectives. This method had been instrumental in acquiring new knowledge about the topic since it allowed participants to elaborate and freely discuss their views, reasonings, and experiences. Talking directly to the experts has provided a better context and thorough explanations of how GDPR affected their usage of customer analytics in their day-to-day operations. The interview guide questions for professionals mainly focused on how data is used in e-commerce and what changes happened in their systems/operations following GDPR compliance, if any. Meanwhile, the guide questions for the customers concentrated on whether they were aware of the law, and how (and if) their trust and willingness to share data after GDPR changed. Additional and follow-up questions

were also asked depending on the participant's background and experience. For ethical considerations, the informants signed written consent in this research. All informants' names and their respective organizations are anonymized (by default).

3.2. Informant Selection

In total, ten semi-structured interviews were conducted with informants. Five with e-commerce professionals, and five with e-commerce clients. The duration of the professional interviews ranged from 35 to 50 minutes and was conducted via Zoom. Prospective participants were initially contacted through LinkedIn. The selection of interviewees is based on their area of expertise, knowledge, background, and expected contribution to answering the research questions. Besides that, all participants should have at least three years of experience working in the e-commerce industry in the Netherlands since GDPR was implemented in May 2018. Table 1 below outlines an overview of the professional e-commerce informants.

Table 1: Overview of informants: E-commerce Professionals.

Code for reference	Job Title/Position	Company Description
EP1	E-commerce Manager	Dutch low-price retail store for clothing and textiles
EP2	Lead Web Analyst	A global online food delivery company operating primarily in Europe
EP3	Senior Data Analyst	Danish fashion company with both offline and online stores
EP4	Senior Analytics Manager	American shoes and sports apparel retailer with both offline and online shops
EP5	E-commerce Coordinator	Global sports equipment and apparel company with operations in the US, Europe, and Asia

As above-mentioned, five interviews were conducted with consumers who experienced buying products and services online. The duration of the client interviews ranged from 25 to 40 minutes and was conducted either face-to-face or via phone interview. The customer participants recruited for this research are individuals living in the Netherlands, either a student or a young professionals. Four out of five respondents also shared that they shop online at least twice a month. The overview of customer informants is illustrated in Table 2.

Table 2: Overview of informants: Customers.

Code for reference	Age	Gender
CP1	26	F
CP2	30	M
CP3	26	F
CP4	26	M
CP5	30	M

3.3. Data Analysis

The data obtained were transcribed for data analysis. After which, coding was introduced to interpret the interviews. The coding approach effectively identified common concepts and themes relevant to answering the research questions. Inductive coding is deemed an appropriate method to organize the findings from the interviews since it provides a simple and direct method for stemming findings linked to focused evaluation questions [3]. Furthermore, inductive coding allows the researchers to perceive new and significant outcomes that can go beyond the preconceptions or expectations imposed on deductive coding. The authors read and analyzed the transcripts to identify and label

categories. Phrases and keywords were selected and highlighted in conceptualizing into central themes. The following section presents the findings identified in the coding process.

4. Findings and Discussion

This section summarizes the findings generated from the interviews conducted. It describes and analyzes prevalent ideas and concepts relevant to answering the research questions. This section also discusses significant findings which are related to existing literature.

4.1. Data

The paramount importance of data has become the central theme in the conversations with the research participants. It is *somehow* not surprising, as GDPR's primary aim is to protect data in all its lifecycle, and e-commerce companies used to collect vast amounts of data from various sources to analyze. The e-commerce professionals explained that they mainly use three key data types in their day-to-day operations: order information, behavioral information, and customer information. Naturally, when a customer places an order on the website or mobile application, companies receive data about their purchases. E-commerce companies gather this information from customers, suppliers, and other stakeholders to coordinate necessary steps in the order fulfillment process. Efficient order management not only reduces costs but also leads to a seamless customer experience, which in turn results in customer retention and increased revenue. Therefore, it is not surprising when companies deem order information as the foundation of their operations. Aside from order information, companies highly value user behavior information in their systems. Online user behavior refers "to the characteristics and behavior of site visitors that is described and reflected in web analytics data" [30]. EP2 stressed the importance of acquiring users' behavioral data as it '*can be used for experimentations, basic product optimization, control for monitoring, and many more'.* EP1 revealed that their data collection process '*already starts even if the customer still has not bought anything yet; it started with placing a pixel'.* According to Hu, et al. [31], the pixels are designed to automatically load from a remote server via HTTP/HTTPS protocols and give a signal to the sender's website once the user comes across the ad or opens their promotional emails. As EP1 highlighted, pixels are responsible for tracking customers' interaction with their marketing emails and ads on social media sites such as Facebook, YouTube, TikTok, etc. Moreover, the utilization of pixels can provide actual numerical values that could be used for statistical testing of a web page design, or a monetary value for online retailers' websites and aligns the website changes directly to KPIs achievements [32]. In addition, e-commerce companies look at other user-behavior information from cookies and session recordings. Finally, the consumer information contains their personal data and what is categorized as *sensitive data* by GDPR. Hence, this data is deemed the most confidential type of data e-commerce companies gather. It may include the customer's name, email address, phone number, location, birth date, gender, etc. Most of our professional participants indicated that because of the sensitive information that their firms collect, the security of this data is much stricter than other parts of the system. When employees extract this data, it is encrypted to prevent it from being traced back to individuals. To improve their products and services, e-commerce companies also ask for other data types, such as customer feedback through surveys and reviews. EP4 shared that '*as soon as someone places an order, they get a survey asking what their experience was like?*' All this information is used to gauge the performance of their website and make significant adjustments to their page.

4.2. Data Collection and Processing

As highlighted in section 2, the GDPR regulation intends to limit the operations on personal data collected from customers. In other words, organizations should only ask for relevant data in fulfilling their operations, which comply with regulations. First, companies reevaluated all the procedures related to storing and processing data. EP2 and EP4 detailed how their respective companies initially assessed their current processes and compared them against the security standards of the regulation. Other participants also discussed how they consolidated all their data into one central data warehouse, wherein all data users are mapped together for effective communication in detailing proper documentation of data-related processes. To make all this possible, interview participants noted the legal departments being heavily involved in data processes' negotiations and discussions. Firms also started to scrutinize the current and

historical data they "own." As EP1 noted, '*GDPR dictates that you only collect data that could be useful or is useful instead of everything.'* Furthermore, companies should only collect data when they have permission from the customers to do so. Thus, redesigning their websites to obtain informed consent from customers is a fundamental step towards GDPR compliance for online businesses. Moreover, the companies prioritized updating their terms and conditions to notify customers about how their data is used and processed. Customer interviewees agree that e-commerce companies improved their communication of data collection processes with their stakeholders. According to CP2, '*the communication of what is collected, how it will be used and the choices I have in this process show while interacting with these businesses online*.' Additionally, CP4 mentioned how '*consent is explicitly requested, and all details pertaining to the consent are explicitly stated'*. Now, companies consider the customers' preferences by giving them options to customize circumstances under which they would disclose their personal information. To conclude, customers seemed rather indifferent to sharing their personal information despite the knowledge of the data collection purposes of e-commerce companies.

4.3. E-commerce Strategies and Tools

Data is considered an asset in any organization. However, data without context is hard to interpret, which is why e-commerce companies adopt different technologies and strategies to understand and interpret data. In line with this, e-commerce experts talked about numerous e-commerce analytics tools they use, depending on their job responsibilities. Furthermore, the widely used techniques in e-commerce were often referred to in illustrating the advantages of incorporating e-commerce analytics in their processes. Companies frequently discuss Google Analytics' reports in their day-to-day activities. Google Analytics reports provide web metrics to evaluate users' shopping behaviors. Aside from shopping behavior, various e-commerce reports can also be generated from this tool, such as relationships between marketing campaigns, user engagement, purchase activity, conversion rates, etc. All of which are relevant in the informed decision-making of e-commerce companies to improve customer experience. For data visualization and reporting tools, Tableau, Python, PowerBI, and Excel were often mentioned by the interview participants. For EP3, it is equally important to understand the data collected and turn them into insights. These tools are beneficial for simplifying results from the analysis and presenting them to managers, other employees, and relevant stakeholders.

4.4. Usage of e-commerce analytics tools after GDPR

As mentioned above, the amount of data e-commerce companies collect has been reduced following the GDPR activation. Thus, it is not surprising that Engan [23] concluded that the new regulation would restrict the ability of firms to drive value from their previous analytics solutions and other algorithmic decision-making systems. E-commerce companies had contrasting views when asked about the impact of GDPR on their analytics operations. For example, companies started to revisit their contracts with their partners in data collection and processing. The GDPR dictates that a data processing agreement (DPA) should be arranged if the company avails the services of a third party when processing customers' personal data. This document ensures that the third-party service provider has adequate security measures to protect the most sensitive information. EP1 supposes that any changes in e-commerce analytics systems will depend on the company's setup. While it certainly limited the data that can be collected and used, his company did not observe a considerable negative impact on their analytics efforts. As he puts it, *'it limited the use of data. But no, it did not limit the success of Big Data. It is about behavior. It is how you use the tools. If you use them wisely and smartly, you can still get everything out of it that you want'.* In this regard, how they use their tools and technologies stayed the same. On the brighter side, customer participants revealed they do not feel the least concerned when their data is used to improve the accuracy of machine algorithms in making personalized recommendations. For CP3, '*I prefer to see personalized marketing content because they are more likely to be something I am interested in'.* Similarly, CP5 noted, '*I prefer the recommendations from the machine algorithms since it will help me order the products I want or need'*. However, CP4 emphasized that he is all right with these technologies only if the number of recommendations is not too much. To conclude, customers trust that adequate security measures are applied to each algorithm to ensure the privacy of the users' data.

4.5. Difficulties and Challenges

Companies consider three main critical concerns in their operations that could be affected by GDPR: 1) *marketing*, 2) *hiring experts,* and 3) *regulatory measures* in different countries. Companies highlighted the impact of GDPR on online advertising and marketing operations. Participants revealed that advertising effectiveness could suffer when asked about the limitations e-commerce companies may experience because of this regulation. Since GDPR stipulates people's privacy rights in every company's data collection process, some customers reject cookies by default. Thus, making it hard to track and monitor website user behavior. When a user interacts with a website, data including browsing history, search queries, transactions, device information, location details, etc., are added to the cookie [33]. EP3 comprehends the need to regulate cookies. However, she also voiced out how this can be a challenge for companies: 'when people reject cookies, of course, you are respecting the decision and privacy of the user. Though this means missing insights, and it can be difficult to make decisions to allocate different budgets or to know if our ad campaigns are working accordingly'. After GDPR, e-commerce companies estimate that around 10-20% of people currently reject cookies. The previous statement is consistent with how the consumer participants perceive cookies. Some informants noted that they do not read what is written in cookie banners and simply click the accept button (as most customers). CP2, on the other hand, had a different behavior: *'I often reject cookies but accept cookies once I have read through the overview and see that accepting them will improve my experience on the website. Therefore, I mostly accept cookies on websites with options to only accept cookies for functional reasons and opt out of marketing ones'*. When asked why this was, he mentioned some advertisements are 'spammy and intrusive'. Adopting GDPR may increase costs at organizations [7]. Extensive training and human resources are among those costs. In line with this, interview respondents shared their experience of taking training and seminars to understand GDPR comprehensively. Furthermore, larger companies assemble GDPR teams in their organizations, and their core obligation is to support their organizations in complying with the regulations.

4.6. Data Management and Security

GDPR aims to bridge the gap between outdated data privacy laws and the rapid shift to the digital economy. This imbalance is why some e-commerce experts suggest that GDPR is 'too late' to be implemented. EP1 explained that *'design principles on which the new technology-based are often not taking the customer in mind from day one.'* Now that GDPR is enforced, it ensures proper measures are embedded by design in every business' IT infrastructure. Likewise, other participants deemed GDPR to be necessary. Before, companies were free to make business choices concerning data without worrying about the potentially harmful effects on society. For that reason, EP4 thinks GDPR '*makes sense and formalizes the normal way of dealing with data'*. In addition, EP5 explains that '*with the kind of personal data that we gather, I understand that we have to be extra careful with it'*. In this regard, GDPR provides rules that guide companies in the proper ways of handling data. Companies shared how they upgraded some of their systems and ensured that only the authorized personnel had access to their most sensitive data. EP1 discussed how they reduced using third-party data and explained that '*we thought whatever data it is, we can use it. But now, we are moving it to first-party data to show that we have ownership of and access to data, instead of everyone'*. Regular audits and continuous discussions with the legal department have become the common practice of the companies. Most of the participants also mentioned properly encrypting their customer data to eliminate the identification of users. From these statements, it is clear how companies still need to be more transparent about their efforts to safeguard customer data.

4.7. Continuous Learning and Future Developments

If e-commerce professionals summarized GDPR compliance in two words, it would be 'continuous learning'. In research by Li [34]. GDPR compliance is described as continuous integration. It is also important to note that companies consider not only GDPR but also other data privacy regulations in every country they operate. Hence, companies make significant efforts to improve their IT infrastructures even after GDPR has been implemented for over three years. Some interview participants shared how their respective companies often go beyond what is stipulated in GDPR and create projects to protect customer data. Technology evolves, and so are data protection laws.

E-commerce professionals revealed they are always on the lookout for updates from the government to ensure they comply with at least the minimum legal security standards in their processes. Interview participants view this as a standard occurrence. EP2 asserted that 'we need to take better care of data; we need to document better what we do with the data; we need to stick to certain regulations.' Hence, e-commerce companies should always be prepared to make necessary system adjustments. Besides that, there is now constant communication with the legal departments at the organizations to discuss important issues concerning their data maps and inventories. Employees develop different solutions to safely implement their marketing campaigns and other projects with these consultations. Whenever there is a new proposal, companies still need to undergo comprehensive planning to follow the guidelines set by the government. Thus, companies view GDPR compliance as ongoing progress, not a one-time requirement.

5. Conclusion

This research investigated the influence of GDPR on BDA systems and other related practices of e-commerce companies in the Netherlands. Various studies were conducted to measure the impact of GDPR on the e-commerce industry. Still, this literature is mainly quantitative and focused on changes in online sales, net margins, operating costs, and other numerical indicators of e-commerce companies before and after the regulation enforcement. On the other hand, via qualitative semi-structured interviews with e-commerce professionals and customers, this paper focused on understanding the impact of adopting GDPR on big data analytics' operations in Dutch e-commerce companies to bridge the literature gap. Meaningful insights were drawn from informant groups, professionals, and customers, to confirm the earlier quantitative findings on the GDPR's influence on e-commerce companies. Before this privacy law enforcement in 2018, there were many pessimistic predictions of the impact of GDPR on online businesses, especially for data-driven firms, as the e-commerce industry relies heavily on data and BDA. Thus, it is surprising that e-commerce professionals find the impact of GDPR minimal on their data-related processes and overall business operations. The informants regard GDPR as a necessary tool, considering the exponential prevalence of the Internet of Things (IoT) and big data. In addition, the findings suggest that the regulation enhanced firms' data management and security and enhanced customers' trust and confidence. GDPR was not meant to punish corporations but to help them improve and organize their data collection and handling processes. Overall, the regulation served as the framework for cultivating the practices, values, and experiences of people working with data. Companies have since developed a strong sense of responsibility to foster a culture that values data protection and respects their customers' privacy. And finally, GDPR has been perceived as instrumental in informing customers of their rights and control over their data.

References

[1] E. Cramer-Flood, "Global Ecommerce Update 2021. Insider Intelligence. ," 2021. [Online]. Available: https://www.emarketer.com/content/global-ecommerce-update-2021#page-report.
[2] D. Coppola, "E-commerce in the Netherlands - statistics & facts," 2021. [Online]. Available: https://www.statista.com/topics/4909/e-commerce-in-the-netherlands/#dossierKeyfigures.
[3] S. Yasiukovich and M. Haddara, "Social CRM in SMEs: A Systematic Literature Review," Procedia Computer Science, vol. 181, pp. 535-544, 2021.
[4] M. Haddara and X. Ye, "Factors affecting consumer-to-consumer sales volume in e-commerce," in Proceedings of the Future Technologies Conference, 2019: Springer, pp. 631-643.
[5] V. Paliwal, "Getting Ready for the European Union's General Data Protection Regulation? Learn, Think and Prepare," 2016. [Online]. Available: https://securityintelligence.com/getting-ready-for-the-european-unions-general-data-protection-regulation-learn-think-and-prepare/.
[6] N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, "Privacy issues and data protection in big data: a case study analysis under GDPR," in 2018 IEEE International Conference on Big Data (Big Data), 2018: IEEE, pp. 5027-5033.
[7] K. Xuereb, S. Grima, F. Bezzina, A. Farrugia, and P. Marano, "The impact of the general data protection regulation on the financial services' industry of small European states," 2019.
[8] G. Aridor, Y.-K. Che, and T. Salz, "The economic consequences of data privacy regulation: Empirical evidence from gdpr," NBER working paper, no. w26900, 2020.
[9] S. Goldberg, G. Johnson, and S. Shriver, "Regulating privacy online: An economic evaluation of the GDPR," Available at SSRN 3421731, 2019.

[10] L. Kuleshova, V. Mukhametshin, and A. Safiullina, "Applying information technologies in identifying the features of deposit identification under conditions of different oil-and-gas provinces," in Journal of Physics: Conference Series, 2019, vol. 1333, no. 7: IOP Publishing, p. 072012.
[11] L. Schmidt, R. Bornschein, and E. Maier, "The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes," Psychology & Marketing, vol. 37, no. 9, pp. 1263-1276, 2020.
[12] S. Balla, "The General Data Protection Regulation and the Privacy Paradox: an exploratory study. ," Erasmus University Rotterdam, 2017. [Online]. Available: https://thesis.eur.nl/pub/41542/Balla-S.-369613.pdf
[13] G. D. P. Regulation, "General data protection regulation (GDPR)–official legal text," Gen Data Prot Regul, 2016.
[14] J. Phillips, Ecommerce analytics: analyze and improve the impact of your digital strategy. FT Press, 2016.
[15] M. Haddara, K. L. Su, K. Alkayid, and M. Ali, "Applications of big data analytics in financial Auditing-A study on the big four," 2018.
[16] S. Akter and S. F. Wamba, "Big data analytics in E-commerce: a systematic review and agenda for future research," Electronic Markets, vol. 26, no. 2, pp. 173-194, 2016.
[17] Z. Fayyaz, M. Ebrahimian, D. Nawara, A. Ibrahim, and R. Kashef, "Recommendation systems: Algorithms, challenges, metrics, and business opportunities," applied sciences, vol. 10, no. 21, p. 7748, 2020.
[18] B. Smith and G. Linden, "Two decades of recommender systems at Amazon. com," Ieee internet computing, vol. 21, no. 3, pp. 12-18, 2017.
[19] T. M. Le and S.-Y. Liaw, "Effects of pros and cons of applying big data analytics to consumers' responses in an e-commerce context," Sustainability, vol. 9, no. 5, p. 798, 2017.
[20] L.-L. B. Wu and D. Wu, "Dynamic pricing and risk analytics under competition and stochastic reference price effects," IEEE Transactions on Industrial Informatics, vol. 12, no. 3, pp. 1282-1293, 2015.
[21] R. K. Mitei, "Revenue Management Practices In the International Airline Industry within Kenya: A Case Study of Air France-KLM Group," United States International University-Africa, 2017.
[22] R. Jhangiani, D. Bein, and A. Verma, "Machine learning pipeline for fraud detection and prevention in e-commerce transactions," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019: IEEE, pp. 0135-0140.
[23] M. Engan, "Big Data and GDPR," University of Stavanger, Norway, 2017.
[24] O. A. Ajibade, "A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape," 2018.
[25] M. Rhahla, S. Allegue, and T. Abdellatif, "Guidelines for GDPR compliance in Big Data systems," Journal of Information Security and Applications, vol. 61, p. 102896, 2021.
[26] J. Schmitt, K. M. Miller, and B. Skiera, "The Impact of Privacy Laws on Online User Behavior," arXiv preprint arXiv:2101.11366, 2021.
[27] A. Bryman, Social research methods. Oxford university press, 2016.
[28] R. K. Yin, Qualitative research from start to finish. Guilford publications, 2015.
[29] D. R. Thomas, "A general inductive approach for analyzing qualitative evaluation data," American journal of evaluation, vol. 27, no. 2, pp. 237-246, 2006.
[30] S. Goldberg, G. Johnson, and S. Shriver, "Regulating privacy online: the early impact of the GDPR on European web traffic & e-commerce outcomes," Available at SSRN, vol. 3421731, 2019.
[31] H. Hu, P. Peng, and G. Wang, "Characterizing pixel tracking through the lens of disposable email services," in 2019 IEEE Symposium on Security and Privacy (SP), 2019: IEEE, pp. 365-379.
[32] A. Brown, B. Lush, and B. J. Jansen, "Pixel efficiency analysis: A quantitative web analytics approach," Proceedings of the Association for Information Science and Technology, vol. 53, no. 1, pp. 1-10, 2016.
[33] T. Zabawa. G. V. S. University. (2020). The Internet and Web Tracking.
[34] Z. S. Li, "Complying with the GDPR in the Context of Continuous Integration," 2020.