

A Comparative Analysis of Data Protection in E-commerce B2C Contracts in Georgia and the European Union

Nato Gugava

PhD, Associate Professor, Faculty of Law, Sulkhani-Saba Orbeliani University; correspondence address: K. Kutateladze Str 3, 0186, Tbilisi, Georgia; e-mail: nato.gugava@sabauni.edu.ge

 <https://orcid.org/0009-0001-8191-6170>


Lika Kobaladze

PhD Candidate, Affiliated Assistant, Faculty of Law, Sulkhani-Saba Orbeliani University; correspondence address: K. Kutateladze Str 3, 0186, Tbilisi, Georgia; e-mail: l.kobaladze@sabauni.edu.ge

 <https://orcid.org/0000-0003-1800-8185>


Tamta Kenia

PhD Candidate, Affiliate Assistant, Faculty of Law, Sulkhani-Saba Orbeliani University; correspondence address: K. Kutateladze Str 3, 0186, Tbilisi, Georgia; e-mail: t.kenia@sabauni.edu.ge

 <https://orcid.org/0000-0003-0226-0247>

Oliko Kobakhidze

PhD Candidate, Affiliate Assistant, Faculty of Law, Sulkhani-Saba Orbeliani University; correspondence address: K. Kutateladze St 3, 0186, Tbilisi, Georgia; e-mail: o.kobakhidze@sabauni.edu.ge

 <https://orcid.org/0000-0003-2012-2286>

Keywords:

e-commerce,
personal data
protection,
digital consumers
rights,
B2C contracts,
legal protection
of e-commerce,
consumers
data security,
regulatory
framework,
institutional
oversight

Abstract: Development of technologies is a great human achievement. Online portals, mobile applications and digital platforms allow citizens to receive services remotely, which, on the one hand, reduces necessity of on-site visits and bureaucratic procedures, however, on the other hand, increases the risk of personal data disclosure processed in such manner. Digital tools play significant role in the process of E-commerce, especially in improving efficiency and accessibility of communication between the consumer and the trader. A lot of people communicate with the extensive use of the internet and technologies, including e-procurement, which, in these relationships require the correct processing of personal data, whereas improper protection of great deal of information increases risks of using data for criminal purposes and threatens personal privacy of consumers. Hence, it is important that organizations providing the internet

services, especially those involved in e-commerce business, be well aware of obligations they are imposed by law. It is worth noting, that Law of Georgia “On Personal Data Protection” was adopted by Georgia in 2011, and its renewed version is quite similar to General Data Protection Regulation of Europe (DGPR) – which was adopted on June 14, 2023 and will enter into force on March 1, 2024. Within changes, the existed standard for personal data processing/protection will be substantially improved. As for protecting personal data processed on the basis of the B2C contracts concluded in the process of E-commerce, the interest regarding these topics increased after spread of coronavirus (Covid-19), when country faced new challenges. This issue is relevant even in the present time, since staying current with technological and legal development, renewed legal regulation and Association Agreement between the European Union and Georgia, imposes additional obligations on the country in the process of perfecting the mentioned field. Accordingly, this article will discuss compliance of regulatory framework of processing/protection of Georgian consumers’ personal data in the online contracts with international standards and existing challenges, to assume obligations of the country under the Association Agreement between Georgia and the European Union to implement E-commerce in practice, best practices of European countries in this regard and the perspective, which Georgia should implement in E-commerce process, in order to insure effective protection of consumers’ data security.

1. Introduction

The world is facing radical changes due to the fast development of internet technologies. Online retailing and the use of the services of companies or Internet platforms that provide those services have become very popular due to the accelerated pace of life. On the one hand, in the field of e-commerce, the number of electronically signed sale or service contracts and their specific importance in the development in this regard is increasing day by day.¹ The usage of technology and electronic systems has indeed improved

¹ See: Lloyd J.F. Southern, “The Attraction and Expansion of E-commerce During Recent Economic Downturn,” *Problems and Perspectives in Management* 10, no. 3 (2012): 107–9,

the possibility of data recording/processing and simplified the service process in time, however, at the same time, it has increased the risks of unauthorised access to data. Therefore, some threats have arisen from traders, who collected and stored confidential information and used as means of manipulation of the consumer without the consumer's consent.² This has given rise to the need to bring established practices and national legislative approaches in line with international standards in order to protect consumers' personal data when concluding online contracts.

It is noteworthy that the "Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part," was signed on June 27, 2014, which was ratified by the Parliament of Georgia on July 18, 2014.³ This relationship document is based on the partnership of the parties, their needs and opportunities for mutual assistance. Association Agreement describes details of the common plan for national development within European standards, after the implementation of which Georgia will become a country compatible with EU standards. Under Article 14 of said document, the parties agree to cooperate to ensure a high level of personal data protection in accordance with the European Union, Council of Europe and international legal documents and standards. The document refers to the mandatory reforms that bring peace and stability to the country (human rights, the rule of law, the fight against corruption and transnational organized crime, etc.) and one of the most important points of the agreement – Deep and Comprehensive Free Trade Area (DCFTA) with the European Union, which resulted in the opening of the European market for the sector of products produced and services offered in Georgia. Chapter 6 of Title IV, which is related to Establishment, Trade in services and E-commerce, is entirely devoted to the regulatory framework of cooperation between the parties concerning free trade and e-commerce. As for e-commerce, on June 13, 2023, the Parliament of Georgia adopted

accessed November 23, 2023, <https://www.businessperspectives.org/index.php/component/zoo/the-attraction-and-expansion-of-e-commerce-during-the-recent-economic-downturn>.

² Sonia Balhara, "Consumer Protection Laws Governing E-Commerce," *Law Essentials Journal* 1, no. 4 (April–June 2021): 20.

³ Fully entered into force on July 1, 2016, accessed November 23, 2023, <https://www.matsne.gov.ge/document/view/2496959?publication=3>.

the Law of Georgia on E-Commerce,⁴ which aims at promoting the proper functioning of the internal market by ensuring the free movement of information society services, protecting the rights of consumers in the process of electronic commerce, determining the rights and duties of intermediate service providers and protecting them from the imposition of general monitoring obligations.⁵ Therefore, Article 6 directly stipulates the protection of personal data in e-commerce transactions and, in cases of violation of the above-mentioned, as a basis of the liability to be imposed, is determined by specific norms of the Law of Georgia “On Personal Data Protection”.

However, it should be noted that before the modernization of the above-mentioned legislative acts, as of January 20, 2020, there were already guidance recommendations on protecting personal data in e-commerce transactions.⁶ The document regulated the details of the importance of personal data protection during e-commerce transactions, challenges and important procedures that trade organizations were obliged to protect and implement in practice. The aforementioned manual was a non-binding regulatory document for companies operating in the e-commerce sector, based on the best practice and general requirements of Georgian legislation, however, due to its non-binding nature, it can be said that it failed to create an effective system for personal data protection between the consumer and the trader within the process of e-commerce transactions.

Thus, the article aims to analyze how personal data is protected when B2C contracts are concluded between the consumer and the trader in e-commerce transactions in Georgia, and examine the experience and problems existing in the Georgian legal space in this regard. Based on best practices of the EU, court decisions and comparative analysis, the article shall present perspectives which would contribute to establishing high standards

⁴ Georgian Law No. 3110-XI⁰ of 20 January 2023.

⁵ Georgian Law on E-Commerce, Article 1(3).

⁶ Chantladze Tato et al., “Recommendation – Protecting Personal Data in the process of online E-commerce, thematic recommendations on personal data management during COVID-19 pandemic,” State Inspector Servicedeveloped by United States Agency for International Development (USAID), Document is prepared with Tetra Tech support, 2022, accessed November 23, 2023, <https://old.pdps.ge/cdn/2022/01/personaluri-monatsemebis-dacva-onlain-vachrobis-processshi.pdf>.

of personal data protection when B2C contracts are concluded between the consumer and the trader in e-commerce transactions in Georgia.

2. Standard of Personal Data Processing and Protection in E-commerce Transactions in Georgia and the European Union

E-commerce, called online trading, is generally a trading activity that involves selling a product and/or service online, for non-cash payment and is defined by the Organisation for Economic Co-operation and Development (OECD)⁷ as all transactions related to commercial activity. However, the World Trade Organization (WTO)⁸ defines e-commerce as the production, distribution, marketing, sale or delivery of goods and services by electronic means.⁹

The formation of e-commerce is intertwined with digital society and economy and is caused by ICT (information and communication technology) achievements.¹⁰ Digital society, which operates with tools such as social media and cloud computing, creates the basis of a digital economy and, due to its countless online connections, global economic activities are carried out rapidly and easily.¹¹ Thus, e-commerce is the practice of conducting business through processing digital information and electronic communication technologies,¹² which, on the one hand, allows business entities to

⁷ The OECD's Consumer Policy Advisory Group is the Commission's main forum for Regulations on e-commerce at the global level. It should be noted that electronic commerce is a central element in the OECD's vision of the potential that our interconnected world holds for sustainable economic growth; accessed November 23, 2023, <https://www.oecd.org/about/>.

⁸ "The World Trade Organization (WTO) is the only global international organization dealing with the rules of trade between nations. At its heart are the WTO agreements, negotiated and signed by the bulk of the world's trading nations and ratified in their parliaments. The goal is to ensure that trade flows as smoothly, predictably and freely as possible." WTO, "The WTO," accessed November 23, 2023, https://www.wto.org/english/thewto_e/thewto_e.htm.

⁹ WTO, "Work Programme on Electronic Commerce," WT/L/274, September 30, 1998, accessed November 23, 2023, https://docs.wto.org/dol2fe/Pages/FE_Search/ExportFile.aspx?id=31348&filename=T/WT/L/274.DOC.

¹⁰ Amir Ebrahimi Darsinouei and Rashid S. Kaukab, *Understanding E-Commerce Issues in Trade Agreements: A Development Perspective Towards MC11 and Beyond* (Geneva: CUTS International, 2017), 9.

¹¹ *Ibid.*, 10.

¹² Daksha Jha, "E-commerce and Consumer Protection: Critical Analysis of Legal Regulations," *Indian Journal of Law and Legal Research* 5, no. 1 (2023): 2.

establish themselves in certain markets and, on the other hand, provides online consumers with the convenience to purchase products and services without leaving their offices and homes.¹³

The beginning of the 1990's should be considered the initial stage of e-commerce.¹⁴ As a result of technological development, since the 1990s, the relationship between businesses and consumers has undergone immense changes, it became possible to conclude contracts remotely and online, and the first secure online purchase was made in 1994.¹⁵ Back then, the Internet was still at an early stage of its development and websites known as Web 1.0 resembled online catalogues, providing the consumers only with static content.¹⁶ In the 21st century, the COVID-19 pandemic strengthened and increased online purchases and this tendency continues successfully up to the present day.¹⁷ Thus, undoubtedly, e-commerce provided consumers with maximal convenience in online purchasing and, alongside technological progress, increased protection standards in the Georgian and EU legislation because consumers should be legally protected from possible damage caused by unfair business practices.¹⁸

2.1. Legal Regulation of Personal Data Protection in E-commerce Transactions

In Europe, the legal framework of e-commerce is based on two directives: Directive of the European Parliament and of the Council No. 1999/93/EC on a Community framework for electronic signatures¹⁹ and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic

¹³ Tomáš Peráček, "E-commerce and Its Limits in the Context of the Consumer Protection: The Case of the Slovak Republic," *Juridical Tribune* 12, no. 1 (March 2022): 35.

¹⁴ OECD, "Toolkit for Protecting Digital Consumers. A Resource for G20 Policy Makers," 2018, 11.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Kamaraj Kanagayazhini, "Critical Analysis of Data Protection and Privacy in E-commerce," *Indian Journal of Law and Legal Research* 4, no. 6 (2022–2023): 3.

¹⁸ Rahmi Ayunda, "Personal Data Protection to E-commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform* 18, no. 2 (2022): 145.

¹⁹ Directive of the European Parliament and of the Council No. 1999/93/EC concerning Community framework for electronic signatures (O.J.E.C. L013, 19 January 2000), 12–20, accessed November 24, 2023, <https://eur-lex.europa.eu/eli/dir/1999/93/oj>.

commerce, in the Internal Market (“Directive on electronic commerce”),²⁰ the purpose of which is to encourage the growth of the internal market by maintaining complete independence in the economic market with basic regulations. According to these directives, a common harmonized legal framework was to be created for EU member states. Nonetheless, it could be said that today there is still no common legal framework that would regulate the field of e-commerce not only globally but even within EU countries. Of note, the reason for this is believed to be the lack of the will of states to limit free trade by regulations.²¹

What is more, it should be noted that outside the European Union, the United Nations Organization attempted to regulate e-commerce at the international level in 2005, with the creation of UECIC²² and the World Trade Organization, which adopted a declaration on international e-commerce in 1998.²³ However, none of the above-mentioned documents could serve as an international regulation, as it could not legally stay current with the accelerated development of Internet technologies.

Contrary to what has already been mentioned, it should be said that the flaws of the common regulation of the legal framework of e-commerce are not typical for the legislation regulating personal data protection. Starting with the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 by the Committee of Ministers of the Council of Europe (the so-called Convention 108

²⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce; O.J.E.C. L178, 17 July 2000), 1–16, accessed November 24, 2023, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex-%3A32000L0031>.

²¹ Cf. Brian Bieron and Ahmed Usman, “Regulating E-commerce through International Policy: Understanding the International Trade Law Issues of E-commerce,” *Journal of World Trade* 46, no. 3 (2012): 546, accessed November 24, 2023, https://www.researchgate.net/publication/290752964_Regulating_E-commerce_through_International_Policy_Understanding_the_International_Trade_Law_Issues_of_E-commerce.

²² United Nations Convention on the Use of Electronic Communications in International Contracts, accessed November 24, 2023, https://wipolex-res.wipo.int/edocs/lexdocs/treaties/en/uncitral-uecic/trt_uncitral_uecic.pdf.

²³ United Nations, “UNCITRAL Model Law on Electronic Commerce 1996 with additional Article 5 bis as adopted in 1998,” accessed November 24, 2023, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

(CETS 108)),²⁴ which is the first and only binding international tool in the field of data protection and applies to all types of data processing, completed by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)²⁵ – a set of uniform data protection rules is being created. This directive also applies to the process of data processing in e-commerce. To be fair, it should be noted that the existing legal regulation of personal data protection²⁶ required harmonization²⁷ to ensure a high level of protection of personal data and their free transfer between member states. In the realm of data protection legislation, Germany led the charge by adopting the world's first data protection laws in 1970–1976. Shortly after, in 1973, Sweden followed suit and, in 1977, France also followed this example. The United Kingdom joined this trend by enacting the Data Protection Act in 1984, with the Netherlands following suit in 1989. It is worth noting that the purview of these regulations is extended to encompass the intricacies of data processing within the sphere of e-commerce.

The rapid changes in information technology and the fact that the free movement of goods, capital, services and people in the internal market required the free movement of data, which could not be achieved without an equally high standard of data protection in the member states, led to the need of a reform of the EU data protection legislation, which resulted in the adoption of the General Data Protection Regulation (GDPR). This

²⁴ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981, accessed November 24, 2023, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008db85>.

²⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (O.J.E.C. L119, 4 May 2016), 1–88, accessed November 24, 2023, <https://gdpr-info.eu>.

²⁶ In 1970–1976, Germany adopted the world's first data protection legislation, in 1973 Sweden did the same, in 1977 France followed in their footsteps, the UK adopted the Data Protection Act in 1984, and the Netherlands in 1989.

²⁷ Goshadze Kakhaber and Begiashvili Malkhaz, eds., *European Law on Data Protection*, handbook, translation (Tbilisi: “World of Lawyers”, 2015), 20, accessed November 24, 2023, <https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ka.pdf>.

act regulated and created a common standard for the process of data processing in e-commerce. Unified data protection rules were established with regard to the basic rights of the data subject²⁸ and the principles of data processing,²⁹ the protection of which is important in e-commerce. Organizations faced new obligations to prescribe and define data processing by default when designing a new product or service,³⁰ appoint personal data protection officers,³¹ comply with requirements of the new right of data transfer³² and obey the principle of accountability.

As for the national standard, Georgia started preparing the Association Agreement between the European Union and Georgia in July 2010. In 2011 the topic of Deep and Comprehensive Free Trade Area (DCFTA) was added to the issues,³³ the implementation of which creates a real mechanism for the gradual economic integration of Georgia into the internal market of the European Union. It also involves the gradual convergence of the legislation regulating the trade sphere and institutions with the relevant regulations and administrative mechanisms of the EU. Within the Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part (Article 76, Articles 127–128),³⁴ the parties agree to promote the development of e-commerce, which should be compatible with international standards to ensure the trust of e-commerce consumers.

Thus, with the Association Agreement with the European Union, Georgia has undertaken to bring the legislation into compliance with European standards, including the legal part of personal data protection and e-commerce, which the country is gradually fulfilling. One of the clear examples of the fulfilment of the obligation assumed under the Association Agreement is the adoption of the Law of Georgia on E-Commerce, which will significantly contribute to the deepening of the trade relationship

²⁸ Ibid., Article 15–22.

²⁹ Ibid., Article 5.

³⁰ Ibid., Article 25.

³¹ Ibid., Article 37–9.

³² Ibid., Article 20.

³³ DCFTA, “About Us,” accessed November 24, 2023, <https://dcfta.gov.ge/about-us>.

³⁴ Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part (Article 76, Articles 127–128).

between the European Union and Georgia and the export of goods/services from Georgia to the EU. It is noteworthy that both of the abovementioned directives were fully transposed into Georgian legislation by the Law of Georgia on the Protection of Consumer Rights which entered into force in June 2022 and the Law of Georgia on Electronic Commerce which entered into force in January 2023, and by adopting these new laws, the scope of the contractual or pre-contractual relationship between the consumer and the trader was also regulated accordingly. Like Directive 2011/83/EU, Georgian legislation establishes the scope of the relationship of the consumer with the trader as any natural person who is offered goods or services, or who purchases or further consumes goods or services exclusively for private purposes and not for performing any commercial practice or industrial activity, crafting or other occupational activities.³⁵ Accordingly, the parties to a B2C legal relationship are, on the one hand, a natural person and, on the other hand, a trader, who may be either a natural person or a legal person. In addition, the Law of Georgia on the Protection of User Rights, like the Directive mentioned above, establishes the obligation of the consumer to share personal information only in case of withdrawal from a distance contract.

Moreover, in order to come closer to the European standard, Georgia changed the definition of data subject's consent with the new Law on Personal Data Protection and added to it the definition of electronic declaration of will,³⁶ which will be actively used in the process of implementing the Law on E-Commerce adopted on June 13, 2023. Thus, with the joint application of the said laws, the proper practice of personal data processing in the conditions of e-commerce should be established, which will be supervised by the Personal Data Service.

2.2. Protection of Personal Data Processed in E-commerce Transactions

Protection of the processed personal data of consumers is one of the key issues in the process of e-commerce implementation, because it is necessary to identify a person (e.g. name, surname, date of birth, personal number,

³⁵ Law of Georgia No. 240110010.05.001.020542 of 29 March 2022 on the Protection of Consumer Rights, Article 4(i).

³⁶ Law of Georgia on Personal Data Protection, Article 3(m, n).

citizenship, etc.), confirm their identity and contact data (e.g. address, phone number, e-mail, IP address, etc.) and often – bank and credit information of the counterparty (card data, income information, etc.) in order to enter into an e-commerce legal relationship. As much as special attention is paid to data security and processing in e-commerce, the importance of data protection in electronic legal proceedings should be first considered in this regard.

The Georgian Law on Personal Data Protection (both the one currently in force and the proposed one) establishes general rules and requirements for personal data protection and does not specifically address particular cases of lawfulness of data processing in e-commerce. However, according to the recommendations developed by the Georgian supervisory authorities,³⁷ it is reasonable for the Internet service provider (including the provider of electronic purchases) to have a clear and detailed internal standard for personal data protection, which reflects the specifics of its activities and regulates the rules of personal data collection, data access, storage, destruction and disclosure to third parties.³⁸ Information about the internal standards of the service provider should be available to the consumer through the so-called privacy policy, which would provide detailed information on processing the consumer's personal data when using the website, the period of data storage, the disclosure of data to third parties, and in case of service termination – on the further use of the data and the means of exercising the consumer's rights. On the one hand, the consumer should be enabled to become aware of the application of privacy policy before using the Internet service and express their consent to the processing of their personal data in accordance with the rules and proportionality principles contained in the application.³⁹ Thus, e-commerce providers are bound by a special obligation to provide the security of the personal data of consumers collected during the provision of services, on the one hand,⁴⁰ and not to

³⁷ Recommendations of Personal Data Protection Inspector Apparatus about personal data protection on the Internet, 3, accessed November 24, 2023, <https://old.pdps.ge/cdn/2018/12/Online-Privacy-Rec-for-Users-.pdf>.

³⁸ Ibid.

³⁹ Ibid., 4–5.

⁴⁰ Cf. Balhara, “Consumer Protection Laws,” 20.

process unnecessary and large volumes of data,⁴¹ which is not necessary for the scope of their legal relationship, on the other hand.

As for the legal practice of e-commerce in Georgia, in this regard, the results of planned inspections carried out by the Personal Data Protection Service are worth noting.⁴² During the study of one of the large companies transporting parcels from different countries, the supervisory authority found that the terms and conditions provided on the website did not contain a text of consent through which the consumer would agree to the conditions of processing their data by the company.⁴³ Moreover, during the registration process on the website, the consumer necessarily agreed to the terms and conditions of the company's services, while the document did not contain information about the purpose of processing each type of data requested during the registration process on the website and the rights of the data subject.⁴⁴ Therefore, the fact that the company kept the collected data until the consumer requested to cancel the registration, is also important. Accordingly, from the perspective of data security, the fact that the company did not use the HTTPS protocol for secure transfer of data through the Internet, was considered a violation by the supervisory authority.⁴⁵

In the practice of the Personal Data Protection Service regarding e-commerce, the inspection of a company trading in household goods is also noteworthy.⁴⁶ Within its inspection, it was determined that through the website, technical support from an individual entrepreneur and one of the companies was used in data processing and that these persons had access to the consumers' data processed through the website without the consumers being informed about it.⁴⁷ As part of the inspection, it was also

⁴¹ Cf. Suzanne Mercer, "Data Protection and E-Commerce in the UK," *International Journal of Franchising Law* 4, no. 1 (2006): 22–3, accessed November 24, 2023, <https://www.scribd.com/document/589056306/4IntlJFranchisingL20>.

⁴² Decision of the Head of the Personal Data Protection Service No. g-1/192/2022 of 15 December 2022.

⁴³ *Ibid.*, 15–23.

⁴⁴ *Ibid.*, 19–23.

⁴⁵ *Ibid.*, 20–3.

⁴⁶ Decision of the Head of the Personal Data Protection Service No. g-1/242/2023 of 26 October 2023.

⁴⁷ *Ibid.*, 23–9.

revealed that the security measures of data processing were also violated by the company, in particular, only one consumer with controller rights was registered for the system management of the server which was used by the individual entrepreneur providing technical support for the website and each employee of the limited liability company.⁴⁸

It is noteworthy that the standards of the lawfulness of the processing of personal data of consumers in e-commerce, especially with regard to data security, are gradually improving along with increasing public awareness. This is also addressed by Article 33 of the new Law of Georgia on Personal Data Protection, according to which data processors, including trade organizations, should appoint a person responsible for protecting personal data (data protection officer (DPO)) and provide them with a mandate to implement personal data protection policy. However, for practical purposes, it is also important that an organization involved in e-commerce transactions has developed and implemented such control mechanisms that would ensure the confidentiality and integrity of personal data (for example: when processing personal data, persons authorized by the controls integrated in the IT system, should be granted access only to such personal data whose processing is necessary for the performance of the duties assigned to the person).⁴⁹

Thus, in order to protect personal data processed in e-commerce transactions, service providers are obliged to remain within the framework of the legal relationship to the extent that is necessary and justified based on the legal purposes of information processing. Consequently, in order to provide the protection of personal data collected through contractual relations, it is advisable to appoint a data protection officer, as mandated by Article 26 of the new Georgian Law on Personal Data Protection, which mirrors Article 25 of the GDPR. This officer would be directly responsible for continuously improving the organization's data protection policies, monitoring ongoing data processing activities, and ensuring compliance with the relevant legal requirements. It is imperative that data processing

⁴⁸ Ibid., 27–9.

⁴⁹ Recommendations of State Inspector on: “Processing Of Personal Data In The Process Of Online Shopping,” January 22, 2020, 3, accessed November 24, 2023, <https://www.personal-data.ge/cdn/2022/01/personaluri-monatsemebis-dacva-onlain-vachrobis-processhi.pdf>.

activities are outlined in an equitable and transparent manner, with priority placed on data privacy as a standard. Additionally, relevant technical and organizational measures should be implemented to enhance data coverage and mitigate the risks of security breaches and unauthorized disclosure, as stipulated by the aforementioned legal obligations.

3. Legal Nature of B2C E-contract

The e-contract is the main basis for establishing commercial legal relations in the digital world. It is impossible for e-commerce to exist and develop without e-contracts.⁵⁰ Therefore, the content and features of e-commerce relations are the main tools which make it possible, in general, to define and identify contextual aspects of the e-contract and, specifically, one of its types – the e-contract between the consumer and the trader.⁵¹

It should be noted that the transition to a market economy parallel to the digitalization of society enabled e-commerce to develop in the digital economy and ensured the development of four types of business models: (1) B2B–business-to-business, (2) B2C–business-to-consumer, (3) B2G–business-to-government, (4) C2C – consumer-to-consumer.⁵²

Among the models listed above, the optimal and most common one is the B2C model, regulating contractual relations between business and consumer,⁵³ which significantly differs from the remaining three models. For example, the business-to-business (B2B) model of relations refers to trade relations between two or more entrepreneurs, whereas B2C is a trade model where goods and/or services are transferred directly from the entrepreneur to the final consumer. In the latter case, it is necessary to purchase

⁵⁰ Sean O'Reilly, "E-Commerce and Contract Making," *Irish Business Law Quarterly* 4, no. 3 (2012): 19.

⁵¹ Anabela Susana de Sousa Gonçalves, "The E-Commerce International Consumer Contract in the European Union," *Masaryk University Journal of Law and Technology* 9, no. 1 (2015): 9.

⁵² Sreeramana Aithal, "A Review on Various E-business and M-Business Models & Research Opportunities," *International Journal of Management, IT and Engineering* 6, no. 1 (2016): 275.

⁵³ Sugeng and Annisa Fitria, "Legal Protection of E-Commerce Consumers Through Privacy Data Security," in *Advances in Social Science, Education and Humanities Research*, vol. 549: *Proceedings of the 1st International Conference on Mathematics and Mathematics Education (ICMMEd 2020)*, eds. Trena L. Wilkerson et al. (Atlantis Press, 2020), 277.

goods or services for one's own personal consumption.⁵⁴ The B2C model is the most widespread model of e-commerce which refers to relations between business and consumer in the electronic space and enables the consumer to become acquainted with the information about specific goods, and other consumers' feedback, find the desired products without leaving home, and enter into contractual relations with the seller through the same virtual space.⁵⁵

Even though B2C e-commerce includes relations related to the electronic purchase and sale of goods and services, it also involves two-way communications between the consumer and the trader, which means that besides sharing information about goods and services, the consumer provides the trader with personal data in the contract-making process. Facebook, a popular social media platform, is one of the most illustrative examples of B2C platforms. The variety of activities offered to consumers by this platform, both paid and free of charge (though with advertising materials), make it an immense B2C platform. For example, with regard to case C210/16,⁵⁶ the Court of Justice examined the persons responsible for personal data processing and controllers of the processing and came to the conclusion that Facebook/Facebook fan pages were jointly and severally liable to the consumer, since they provided the service to the consumer through an electronic platform, at the same time, used cookies, without consent, to keep and later use the personal data of the consumer.

Thus, B2C e-commerce can be defined as the provision of remote services and information exchange through electronic means for remuneration between entrepreneurs and final consumers, based on their individual requests.⁵⁷

⁵⁴ Tony J. Jewels and Greg T. Timbrell, "Towards a Definition of B2C & B2B E-commerce," *ACIS Proceedings* 56 (2001).

⁵⁵ Balhara, "Consumer Protection Laws," 19.

⁵⁶ CJEU Judgment of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, ECLI:EU:C:2018:388, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8060600>.

⁵⁷ Jewels and Timbrell, "Towards a Definition."

3.1. Personal Data of the Consumer Processed Under a B2C E-contract

The consumer, compared to the entrepreneur, is a vulnerable and less informed side of the contractual relationship within the framework of e-commerce. In order to eliminate this imbalance, a relatively high standard of information and protection at the legal regulation level is used.⁵⁸ The Law of Georgia on the Protection of User Rights establishes certain mechanisms for protecting natural persons, including the consumer, is obligation to send to the trader a completed form or other clear evidence, which reflects the consumer's decision to return the goods within the established period,⁵⁹ and the trader having no right to request more than the following information to be provided in the form by the consumer for the latter to withdraw from the contract: (a) name, actual address, fax number, e-mail address specified by the trader; (b) date of order; (c) date of receiving the order; (d) consumer name; (e) consumer's address; (f) consumer's signature (if the form is filled out on paper); (g) date of filling out the form.⁶⁰ At the same time, with regard to increased protection of consumers, it is necessary to respect their right to information and protect their personal data, which is confirmed by the clarifications made by the Court of Justice of the European Union⁶¹ (hereinafter CJEU) in a number of essential cases regarding the protection of the rights of consumers as data subjects.

In particular, in this regard, an interesting case examined by the CJEU in 2016 should be mentioned at this point, as it was the first time the court explained the concept of personal data, which is successfully used in all cases of this category, also when protecting personal data in e-commerce transactions.⁶² In this case, Mr Breyer, a German citizen, requested that

⁵⁸ Tamar Lakerbaia, "Definition of the 'Consumer' in the practice of European Court of Justice," *Orbeliani Law Review*, no. 4 (2021): 74.

⁵⁹ Law of Georgia No. 240110010.05.001.020542 of 29 March 2022 on the Protection of Consumer Rights, Article 13(4).

⁶⁰ *Ibid.*, Article 13(5).

⁶¹ Court of Justice of the European Union consists of two major courts: the Court of Justice, informally known as the European Court of Justice (ECJ), which hears applications from national courts for preliminary rulings, annulment and appeals; Court of Justice of the European Union, accessed November 24, 2023, https://curia.europa.eu/jcms/jcms/j_6/en/.

⁶² CJEU Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, accessed November 24, 2023, <https://curia.europa.eu/juris/>

Germany prohibit, or instruct third parties to prohibit the storage of computerized data transmitted at the end of each consumer's consultation/visit to the websites of German federal institutions. Data included information about website access time and the consumer's IP address, which enabled the service provider to identify the consumer. The Court of Justice emphasized that European legislation does not provide for an obligation of one specific person to hold all information that allows the identification of a data subject. Consequently, the court considered the dynamic IP address, registered by the electronic service provider to constitute personal data when the consumer tries to visit a website.⁶³

In 2003, as a result of subsuming actual circumstances within the legal regulations of the European Union, the Grand Chamber of the Court of Justice, with regard to Case C-101/01,⁶⁴ also clarified the concept of personal data processing. In particular, the court noted that specifying a person on the website, identifying them by name or by other means, for example, a phone number or information about their working conditions and hobbies, constitutes the processing of personal data.

It is also noteworthy that the consumer's personal data collected within e-commerce transactions often does not remain solely within the control of the trader with whom the consumer establishes a relationship. For example, the case considered by the Grand Chamber of the Court of Justice in 2015 concerns the disclosure of personal data collected within e-commerce

document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8059289; see also: CJEU Judgment of 20 December 2017, Peter Nowak v. Data Protection Commissioner, Case C-434/16, ECLI:EU:C:2017:994, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8059397>; Court of Justice of the European Union, "Fact sheet on the Protection of Personal Data," 2021, 45–60, accessed November 24, 2023, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf.

⁶³ Ibid.

⁶⁴ CJEU Judgment of 6 November 2003, Criminal proceedings v. Bodil Lindqvist, Case C-101/01, ECLI:EU:C:2003:596, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=305437>; Court of Justice of the European Union, "Fact sheet," 45–60, accessed November 24, 2023, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf.

transactions with a third country.⁶⁵ Regarding this case, Facebook user – Mr Schrems filed against Facebook Ireland, claiming that the user’s personal data were being transferred to the United States of America and stored without adequate safeguards. The Grand Chamber overturned the Commission’s decision regarding this case, noting that the “Safe Harbor” principle does not apply to any transfer of personal data to the US, but only to US self-certified organizations that receive personal data from the EU and the US State bodies are not required to protect them. Therefore, the court stated that because the issue concerned interference with the right to privacy guaranteed by the Charter of Human Rights, it was necessary to establish minimum guarantees so that the persons whose personal data might have been processed should have sufficient safeguards. The need for such guarantees is even greater when personal data is subject to automatic processing at a significant risk of illegal access to them.⁶⁶

So, in order to ensure effective protection of consumers’ personal data, first of all, it is important to identify such data, except for the data normally needed for concluding contracts (for example: name, surname, address, contact information, etc.), as far as, based on the examples of the court decisions mentioned above, it can be said that the realm of the Internet expands the definition of the concept of personal data even more. This is important, on the one hand, for the protection of good faith in business-to-consumer relations and, on the other hand, for promoting smooth functioning in accordance with the internal market law.

3.2. Rights and Obligations of Data Processor in the E-commerce Transactions

The main obligation of data processor is the safe protection of data security. E-commerce security is often defined as “the protection of an information resource from threats and risks over a network within the confidentiality, authenticity and integrity of transmitted electronic transactions.” E-commerce can only develop if the system can provide the same level of trust and security as that provided in traditional business methods. This can be

⁶⁵ CJEU Judgment of 6 October 2015, Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650, accessed November 24, 2023 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&dclang=EN&mode=lst&dir=&occ=first&part=1&cid=8061186>.

⁶⁶ *Ibid.*, para. 91.

achieved as long as e-commerce consumers are confident about the protection provided in e-commerce.⁶⁷

In e-commerce transactions, the consumer provides their personal information, including personal identifiable information (name, surname, address, phone number, personal number, e-mail), financial history, health information, etc., to a specific website at the pre-contractual or contractual stage, exposing themselves to a breach of confidentiality and this is where the issue of consumer trust in the trader emerges.⁶⁸ In general, online traders create detailed profiles of consumers based on their online activities, where consumers, often very willingly, share their personal data, whereas traders control these data with implicit methods, such as cookies, often without clear consent.⁶⁹ Essentially, there are three basic methods of collecting consumers' data in legal literature: (1) Consumer's data could be shared by the consumer themselves, for example: by creating a social media profile or providing credit card information when making online purchases; (2) Data could be collected with implicit method, when the data subject's role is passive; for example: location sharing with mobile phones or websites; (3) And, finally, based on an individual's financial history, a trader might collect personal data from seemingly "anonymous" or "non-personal" data.⁷⁰

Additionally, the EU General Data Protection Regulation (GDPR) requires vendors involved in e-commerce to align their trading policies with the standards for consumer confidentiality and personal data protection established by the abovementioned regulation.⁷¹

Legislation has stipulated that data processors should use consumer's personal data purposely. In this regard, the practice established by one of the largest entrepreneurs, Amazon, is quite remarkable. In September 2000, Amazon.com, which held the personal data of almost 23 million users

⁶⁷ Balhara, "Consumer Protection Laws," 21.

⁶⁸ Mayank Singhal, "Cross Border Data Protection and E-Commerce," *RGNUL Financial and Mercantile Law Review* 6, no. 2 (2019): 50.

⁶⁹ Kanagayazhini, "Critical Analysis," 3.

⁷⁰ OECD, "Toolkit for Protecting Digital Consumers," 41.

⁷¹ Ashok R. Patil and Akshay Yadav, "Suggested Legal Framework for Strengthening the Consumer Protection in E-Commerce Transactions," *Journal of Law, Development and Politics* 12, no. 206 (2022): 213.

registered on the website, made changes in its confidentiality policy. Afterwards, the consumers observed different prices of the same goods depending on location and browser. Amazon explained this as a price test, which analyzed consumers' online purchase behavior based on price changes. However, critics found specific patterns suggesting that consumers with higher spending habits were offered higher prices than the newly registered or low-budget consumers who were offered lower prices. This discrimination was linked to using cookie files. The consumers deleting or blocking cookie files received larger discounts, which highlighted potential flaws of internal, secondary use of personal data.⁷²

Regarding B2C contracts, a recent case of a Romanian telecommunications firm "Orange" is also of interest to this study. The state sued the company for its unauthorized storage of hard copies identifying its consumers.⁷³ Despite the fact that the Romanian company presented the consumers' consents (in the form of a checkbox) obtained while concluding contracts, the court did not recognize the collection of personal data as legal and explained that in B2C relations, consumer' written consent alone is not enough, if it is not presented in an understandable and easily accessible form. The terms should be stated in a way that enables the consumer to make a free choice, the contractual terms should not mislead them about the possibility of contract conclusion, even if they refuse to give a consent about their personal data processing.⁷⁴ The court did not consider the pre-marking of the consent option by the data controller/person responsible for the processing of personal data during contract conclusion, or the obligation for the consumer to express their opinion in writing in the case of refusal, as an expression of legally valid will by the consumer and found such methods of collection of personal data to be illegal.⁷⁵ During one of the cases, the Grand Chamber of the Court of Justice did

⁷² Priya Singh, "Consumer Privacy in E-commerce," *Supremo Amicus* 25, (2021): 242.

⁷³ CJEU Judgment of 11 November 2020, *Orange Romania SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, Case C-61/19, ECLI:EU:C:2020:901, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?jsessionid=341365AF1A5CF8612998306109611D26?text=&docid=233544&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=40182213>.

⁷⁴ *Ibid.*, paras. 49–51.

⁷⁵ *Ibid.*, para. 52 and following.

not recognize as legally valid consents in which a service provider marks the consent option in advance, and in which the consumer should unselect the consent that has been marked in advance, or submit a written refusal about the consent marked in advance by service provider.⁷⁶

It should be noted that e-commerce companies, according to GDPR provisions, in addition to being required to obtain the consent of consumers for the collection, storage and processing of their personal data, must also allow consumers to exercise full control and gain ownership of their data. This refers not only to European companies but also to foreign companies which have access to EU citizens' personal data. GDPR provides the "Right to be forgotten", right to limit processing and the right to data disclosure, which provide the confidentiality of the consumer in e-commerce platforms.⁷⁷ Indeed, one of the recent decisions in favour of consumers in e-commerce was made by the European Court of Justice (CJEU) and found that consumers whose data was collected in e-commerce transactions on a website or in an online shop have the right to correct the relevant information or, if necessary, delete it (de-referencing of personal data).⁷⁸ Granting consumers with this right should be considered a substantial step forward and one of the mechanisms for protecting e-commerce contracts.

Besides, GDPR makes it essential that data processors should process data legally, fairly and transparently.⁷⁹ Protection of the above-mentioned principles within the framework of such contractual relations, where the consumer is considered as the less informed side of the contract, is particularly important, because not only the proper functioning of the market, but also the reliability of the sharing of personal data of the contractual parties must be protected. It is significant that the current edition of the Law of

⁷⁶ CJEU Judgment of 1 October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH, Case C-673/17, ECLI:EU:C:2019:801, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8062181>.

⁷⁷ Singh, "Consumer Privacy," 243.

⁷⁸ CJEU Judgment of 24 September 2019, GC and Others v. Commission nationale de l'informatique et des libertés (CNIL), Case C-136/17, ECLI:EU:C:2019:773, accessed November 24, 2023, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8061825>.

⁷⁹ Ayunda, "Personal Data Protection," 151.

Georgia on Personal Data Protection also provides for the necessity to process data fairly, legally and without infringement on the dignity of the data subject, although the new law, like the GDPR, establishes such a principle of data processing as transparency, which emphasizes the transparency and perceptibility of the entire process of data processing for the data subject,⁸⁰ which also refers to data processing within e-commerce.

4. Rights of the Supervisory Authority with Regard to Personal Data Processed in E-commerce

Each country of the European Union has a Data Protection Authority (DPA), which is responsible for the execution of the regulation (GDPR) in its member state and is entitled to perform investigative, punitive and supervisory functions. In the case of a violation of personal data processing rules, it is entitled to study the issue, detect the violation, and take appropriate legal measures to resolve the problem.⁸¹ Therefore, measures taken by DPA include imposing a fine, ordering the collected personal data to be destroyed, issuing a warning to bring the process of collecting personal data in compliance with the law, liquidating the offender's business, etc.⁸²

As for the supervision of the lawfulness of personal data processing in e-commerce transactions, the main function of the Data Protection Authority in this regard is to determine whether the rationale for data processing exists and if so, whether the processing complies with internationally recognized principles of personal data protection. Also, the function of the Data Protection Authority is to scrutinize the measures taken to ensure the security of personal data processed in e-commerce transactions.⁸³ As a sanction for the infringement of personal data revealed

⁸⁰ Georgian Law No. 010100000.05.001.016606 of 28 December 2011 on Personal Data Protection, Article 4(a).

⁸¹ Ibid.

⁸² EDPB Guidelines on the GDPR, especially the guidelines on the DPIA and guidelines on data breach notifications, accessed November 24, 2023, <https://ec.europa.eu/newsroom/article29/items/611236>, Chapters IV and VI of the GDPR.

⁸³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Articles 51–9, accessed November 24, 2023, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

in cases related to e-commerce, the supervisory authority may also use the non-material damage compensation mechanism. The latest practice of the Court of Justice uses the same approach and sets additional criteria for compensation of damages. In particular, within a 2023 decision,⁸⁴ the court clarified that not all types of personal data violations lead to the right to claim compensation for non-material damages. Rather, in such cases, it is important to prove the fact of private/personal damage. The court also clarified that damage could only be compensated in case of a GDPR violation, material and non-material damage caused by disputed violation and a direct cause-and-effect relation between the violation and the damage caused by it.⁸⁵

In general, the imposition of fines is recognized as the most effective law enforcement mechanism for the protection of personal data in e-commerce transactions.⁸⁶ In the European Union, fines imposed by the competent authorities usually derive from and depend on the degree of personal violation, however, their amounts are substantial and have the nature of so-called punitive damages. For example, France fined Google 50 million euros, alleging that the company violated collecting personal data in e-commerce transactions, as the process was not transparent, the consumers were given inadequate and insufficient information, which is why they were not consents expressed based on the free will of consumers.⁸⁷ Another case is the UK Information Commissioner's Office (ICO) fining British Airways 20 million pounds for illegally disclosing the personal data and financial information of 500,000 consumers.⁸⁸ ICO also fined Marriot International 99 million pounds, as the latter failed to adequately protect

⁸⁴ CJEU Judgment of 4 May 2023, *Österreichische Post*, Case C-300/21, ECLI:EU:C:2023:370, accessed November 24, 2023, <https://curia.europa.eu/juris/liste.jsf?lgrec=fr&td=%3BALL&dan-guage=en&num=C-300/21&jur=C>.

⁸⁵ *Ibid.*

⁸⁶ European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States*, accessed November 24, 2023, https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_en.pdf.

⁸⁷ Administrative Court of Appeal, *France vs. Google*, April 2019, Case 17PA03065.

⁸⁸ ICO, *Penalty Notice*, accessed November 24, 2023, <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf>.

the personal data of 339 million visitors from unauthorized disclosure.⁸⁹ In 2019, in turn, the Luxembourg Data Protection Agency fined Amazon – the e-commerce giant – 746 million euros as Amazon collected and stored consumers’ personal data in an unauthorized way.⁹⁰

At this point, is worth discussing the “one-stop-shop” mechanism, which the GDPR provides as one of the law enforcement mechanisms that “is aimed at organisations that operate in different member states of the European Union or carry out the transmission of personal data in several member states”.⁹¹ In such a case, the lead supervisory authority is authorized to supervise the collection and transfer of personal data collected in e-commerce transactions. The introduction of the “one-stop-shop” mechanism was aimed at simplifying the regulations imposed on businesses and, accordingly, encouraging electronic commerce.⁹² As for Georgia, the Personal Data Protection Service considers statements and complaints related to the lawfulness of data processing through electronic contracts concluded with consumers in e-commerce transactions. Once a violation is detected, the Service imposes a relevant sanction on the data processor, the amount and type of which are regulated by legislation.⁹³ Unlike in the European Union, the amount of fines in Georgia is minimal (not only by European but also by Georgian standards), for example, the largest fine prescribed by law is 6000 GEL, which is almost equivalent to 2000 euros at today’s exchange rate, and fine amount defined

⁸⁹ Marriott International (2019), Information Commissioner’s Office (ICO) – Marriott International, accessed November 24, 2023, https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en.

⁹⁰ Order of the General Court (First Chamber) of 14 October 2021, Amazon.com, Inc. and Others v. European Commission, Case T-19/21, ECLI:EU:T:2021:730, accessed November 24, 2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021TO0019>.

⁹¹ Data Protection Commissioner, “One Stop Shop (OSS): Cross-border Processing and the One Stop Shop,” accessed November 24, 2023, <https://www.dataprotection.ie/en/organisations/international-transfers/one-stop-shop-oss>.

⁹² Andra Giurgiu, Gertjan Boulet, and Paul De Hert, “EU’s One-stop-shop Mechanism: Thinking Transnational,” *Privacy Laws & Business. International Report*, no. 137 (2015): 1–7.

⁹³ Georgian Law No. 010100000.05.001.020936 of 14 June 2023 on Personal Data Protection, Articles 66, 88.

by the GDPR starts from 20 million euros or is estimated at up to 4% of the company's annual income.⁹⁴

In Georgia, there are almost no disputes arising from the contract concluded within e-commerce, among the few practices found in Georgia, we should highlight the decision taken by the supervisory authority on personal data protection against one of the large companies operating in the e-commerce sector, according to which, based on the contract concluded with the consumer in e-commerce transactions, the company (LLC) selling equipment incompletely recorded the data processing process, as well as there was no recording of the actions performed on the data (so-called logs).⁹⁵ Besides the wide scale of violation, one of the largest e-commerce operators in Georgia was fined only 500 GEL (approximately 200 euros).⁹⁶ Also, the decision against one of the largest household goods selling companies operating in Georgia, which was fined 500 GEL, is also very important, as the Personal Data Protection Service determined that in the process of remote service provided to consumers, the company was not able to record personal data obtained during the contract within e-commerce, including data viewing and data removal. Therefore, personal user portals of those who had access to the consumers' personal data were mis-allocated and, in some cases, non-existent, making it impossible to monitor those who had access to sensitive information.⁹⁷ For this category of infringement, in another case, an enormous electronic commerce entity was also fined 500 GEL.⁹⁸

Based on the analyzed material, it can be said that the imposition of fines on companies in Georgia is characterized as an application form, because, first, the income of electronic traders is rather substantial, so

⁹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); O.J.E.C. L119, 4 May 2016), 1–88.

⁹⁵ Decision of the Head of the Personal Data Protection Service of 26 October 2023 No. ზ-1/241/2023.

⁹⁶ Decision of the Head of the Personal Data Protection Service of 26 October 2023 No. ზ-1/242/2023.

⁹⁷ Ibid.

⁹⁸ Decision of the Head of the Personal Data Protection Service of 3 November 2023 No. ზ-1/251/2023.

it is easier for them to pay “imperceptible” and “painless” fines than spend funds and time to create a policy for the protection of personal data. Second, such minor fines might not and cannot restore the violated rights of consumers to the extent to which material and non-material damage is caused to them, which is much more burden some than the fine imposed on the company, which as a consequence is only a formality. In this regard, bringing the Georgian legislation closer to the amount of the sanction in force in the EU would be an important step forward, so that the fine would not only serve as a deterrent but also perform a practical effective function, persuading electronic traders that without developing a policy for the effective protection of personal data of consumers, the sanction imposed on them could be so financially damaging that it would either threaten their operation in the market or damage their goodwill in a way that a large number of consumers would refuse to cooperate with them. It would also be important to include the “one-stop-shop” mechanism in Georgian legislation, which would limit the usage of Georgian jurisdiction as “a black hole”, therefore, regulating the discussed mechanism at the legislative level would enable to bring together in the legal regime such companies, whose activities include the transfer to different countries of personal data obtained within e-commerce.

In this part, it is important to discuss the mechanism of cooperation of supervisory authorities of member states, which ensures a gradual use of regulations within the EU.⁹⁹ This mechanism includes cooperation among commissions, issuance of advisory opinions and resolving disputes among supervisory authorities of member states.¹⁰⁰ Georgian legislation does not consider such a mechanism of personal data protection in e-commerce and integration of it into national legislation is not much needed until Georgia becomes a member state of the European Union. However, it is noteworthy that despite not having a Status, during the European Data Protection Board (“EDPB”) plenary session on June 20, 2023, it decided to grant the supervisory authority of Georgia the status of an observer of

⁹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; O.J.E.C. L119, 4 May 2016), Articles 60–76.

¹⁰⁰ Ibid.

the European Data Protection Board (EDPB) activities. This is very important because the Personal Data Protection Service would be able to observe the practice of the European Data Protection Board in actual mode, including in the scope of the legitimacy of data processing of natural persons within e-commerce and, by analyzing the best practices, implement these approaches within the scope of its own activities.

5. Conclusion

E-commerce and its legal regulation are an innovation for Georgia, as e-commerce is of high interest today and will become even more important in the future, because the growing development of the Internet and digital technologies connect people, businesses, device, data and processes. This enhances the strengthening of the digital economy, implementation of services through electronic means and the transition to online market trading platforms.

As of today, the existing scarce practice and theoretical legal provisions in Georgia clearly define the obligations of the data processor, providing activities to thoroughly protect the consumers' personal data in contracts concluded in e-commerce transactions. Therefore, in case of a dispute, along with the supervisory authority liable for personal data protection, it also determines the issue of applying to the National Competition Agency, prospectively aiming, even formally, to unambiguously and clearly define rules which would not leave any perceptions of not spreading cases about violation of personal data processing rules in e-commerce transactions. Even though the agency considers cases of harm as well as possible harm to the interests of service recipients, which might include violation of the rights of individuals or groups of individuals caused by illegal processing of personal data, it is within the direct competence of the Personal Data Protection Service.

To sum up, it should be noted that the Law of Georgia on Personal Data Protection and Law of Georgia on E-Commerce are new in Georgia's legal space and, at this moment, their joint consideration and analysis make it possible to only discuss the purpose of legislation, to bring national regulatory framework in compliance with international, especially European, regulatory framework standards. However, from a practical perspective, at present, it is difficult to predict its actual potential in reality and

how the importance of personal data protection in e-commerce relations will be perceived in the Georgian trade space, and in this regard, how will it compare to European practice and what major distinguishing trends will appear.

References

- Aithal, Sreeramana. "A Review on Various E-business and M-Business Models & Research Opportunities." *International Journal of Management, IT and Engineering* 6, no. 1 (2016): 275–98.
- Ayunda, Rahmi. "Personal Data Protection to E-commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform* 18, no. 2 (2022): 144–63.
- Balhara, Sonia. "Consumer Protection Laws Governing E-Commerce." *Law Essentials Journal* 1, no. 4 (April–June 2021): 17–24.
- Bieron, Brian, and Ahmed Usman. "Regulating E-commerce through International Policy: Understanding the International Trade Law Issues of E-commerce." *Journal of World Trade* 46, no. 3 (2012): 546. Accessed November 24, 2023. https://www.researchgate.net/publication/290752964_Regulating_E-commerce_through_International_Policy_Understanding_the_International_Trade_Law_Issues_of_E-commerce.
- Chantladze Tato, Elene Sulkhaniashvili Elene, Tsintsiskladze Giorgi, and Jishiasvili Gvantsa. "Recommendation – Protecting Personal Data in the process of online E-commerce, thematic recommendations on personal data management during COVID-19 pandemic." State Inspector Servicedeveloped by United States Agency for International Development (USAID). Document is prepared with Tetra Tech support, 2022. Accessed November 23, 2023. <https://old.pdps.ge/cdn/2022/01/personaluri-monatsemebis-dacva-onlain-vachrobis-processshi.pdf>.
- Court of Justice of the European Union. "Fact sheet on the Protection of Personal Data," 2021. Accessed November 24, 2023. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf.
- Darsinouei, Amir Ebrahimi, and Rashid S. Kaukab. *Understanding E-Commerce Issues in Trade Agreements: A Development Perspective Towards MC11 and Beyond*. Geneva: CUTS International, 2017.
- Data Protection Commissioner. "One Stop Shop (OSS): Cross-border Processing and the One Stop Shop." Accessed November 24, 2023. <https://www.dataprotection.ie/en/organisations/international-transfers/one-stop-shop-oss>.

- DCFTA. "About Us." Accessed November 24, 2023. <https://dcfta.gov.ge/ge/about-us>.
- Giurgiu, Andra, Gertjan Boulet, and Paul De Hert. "EU's One-stop-shop Mechanism: Thinking Transnational." *Privacy Laws & Business. International Report*, no. 137 (2015): 1–7.
- Jewels, Tony J., and Greg Timbrell. "Towards a Definition of B2C & B2B E-commerce." *ACIS Proceedings* 56 (2001).
- Jha, Daksha. "E-Commerce and Consumer Protection: Critical Analysis of Legal Regulations." *Indian Journal of Law and Legal Research* 5, no. 1 (2023): 2.
- Kakhaber, Goshadze, and Begiashvili Malkhaz, eds. *European Law on Data Protection*, handbook, translation. Tbilisi: "World of Lawyers", 2015.
- Kanagayazhini, Kamaraj. "Critical Analysis of Data Protection and Privacy in E-commerce." *Indian Journal of Law and Legal Research* 4, no. 6 (2022–2023): 3.
- Lakerbaia, Tamar. "Definition of the 'Consumer' in the Practice of European Court of Justice." *Orbeliani Law Review*, no. 4 (2021): 74.
- Mercer, Suzanne. "Data Protection and E-Commerce in the UK." *International Journal of Franchising Law* 4, no. 1 (2006): 22–3. Accessed November 24, 2023. <https://www.scribd.com/document/589056306/4IntlJFranchisingL20>.
- O'Reilly, Sean. "E-Commerce and Contract Making." *Irish Business Law Quarterly* 4, no. 3 (2012): 9.
- OECD, "Toolkit for Protecting Digital Consumers. A Resource for G20 Policy Makers," 2018.
- OECD. "Who We Are." Accessed November 23, 2023. <https://www.oecd.org/about/>.
- Patil, Ashok R., and Akshay Yadav. "Suggested Legal Framework for Strengthening the Consumer Protection in E-Commerce Transactions." *Journal of Law, Development and Politics* 12, no. 206 (2022): 213.
- Peráček, Tomáš. "E-commerce and Its Limits in the Context of the Consumer Protection: The Case of the Slovak Republic." *Juridical Tribune* 12, no. 1 (March 2022): 35–50.
- Singh, Priya. "Consumer Privacy in E-commerce." *Supremo Amicus* 25, (2021): 242.
- Singhal, Mayank. "Cross Border Data Protection and E-commerce." *RGNUL Financial and Mercantile Law Review* 6, no. 2 (2019): 50.
- de Sousa Gonçalves, and Anabela Susana. "The E-Commerce International Consumer Contract in the European Union." *Masaryk University Journal of Law and Technology* 9, no. 1 (2015): 5–20.
- Southern, Lloyd J.F. "The Attraction and Expansion of E-commerce During Recent Economic Downturn." *Problems and Perspectives in Management* 10, no. 3 (2012): 104–11.
- Sugeng, and Annisa Fitria. "Legal Protection of E-Commerce Consumers Through Privacy Data Security." In *Advances in Social Science, Education and Humanities*

Research, vol. 549: *Proceedings of the 1st International Conference on Mathematics and Mathematics Education (ICMMEd 2020)*, edited by Trena L. Wilkerson et al., 275–84. Atlantis Press, 2020.

United Nations. “UNCITRAL Model Law on Electronic Commerce 1996 with additional article 5 bis as adopted in 1998.” Accessed November 24, 2023. https://wipolex-res.wipo.int/edocs/lexdocs/treaties/en/uncitral-uecic/trt_uncitral_uecic.pdf.

WTO. “The WTO.” Accessed November 23, 2023. https://www.wto.org/english/thewto_e/thewto_e.htm.

WTO. “Work Programme on Electronic Commerce,” WT/L/274, September 30, 1998. Accessed November 23, 2023. https://docs.wto.org/dol2fe/Pages/FE_Search/ExportFile.aspx?id=31348&filename=T/WT/L/274.DOC.