VILNIUS TECH
Vilnius Gediminas Technical University

14th International Scientific Conference "Business and Management 2024"
May 16–17, 2024, Vilnius, Lithuania

NEW TRENDS IN CONTEMPORARY ECONOMICS, BUSINESS AND MANAGEMENT

ISSN 2029-4441 / eISSN 2029-929X
eISBN 978-609-476-363-2
Article Number: bm.2024.1248
https://doi.org/10.3846/bm.2024.1248

ON THE ISSUE OF PERSONAL DATA PROTECTION IN THE FIELD OF E-COMMERCE: A COMPARATIVE ANALYSIS OF LEGISLATION IN THE BALTIC STATES AND UKRAINE

Mariia PLESKACH

The Institute of Private Law, Mykolas Romeris University, Ateities g. 20, Vilnius, Lithuania

Received 29 February 2024; accepted 10 April 2024

Abstract. This research focuses on a comparative analysis of the legislation on the protection of personal data in the field of electronic commerce between the Baltic States (Lithuania, Latvia, Estonia) and Ukraine. With the rapid growth of e-commerce and the increase in the collection, processing and use of personal data, it is important to assess the legal framework in place to ensure the privacy and security of persons' information. Therefore, given such factors as the steady increase in the number of digital services, electronic applications and online stores, the cross-border nature of e-commerce and the significant deepening of cooperation between Ukraine and the Baltic States, with a focus on strengthening trade and diplomatic relations, it is important to analyze the level of personal data protection in the field of e-commerce in the Baltic States and Ukraine. Through a comparative analysis of legislation in these regions, this study aims to identify differences and similarities, weaknesses and strengths, potential areas for improvement in data protection legislation. The conclusion will contribute to a comprehensive vision of the legal basis and provide knowledge on improving data protection measures in e-commerce.
This article may be of interest to various stakeholders. For example, for researchers, who are studying data protection and e-commerce, lawyers specializing in e-commerce and private law, companies in e-commerce sector, particularly those with cross-border transactions and electronic agreements in the Baltic States and Ukraine, legislators involved in the process of regulating the protection of personal data and persons, who take care about the security of their personal data during online shopping and electronic transactions.

Keywords: personal data, e-commerce, security of persons' information, digital human rights, data protection.

JEL Classification: K22.

1. Introduction

Relevance of research. Modern information and communication technologies (ICT) and digital technologies are the basis for a wide range of opportunities for people. They have become a tool for improving the quality of life, simplifying access to a variety of goods, services, and facilities. In addition, the latest technologies have led to the transformation of the way people trade and, consequently, the emergence of *electronic commerce (e-commerce)* – electronic economic activity that provides a full cycle of business processes, including ordering goods/services, making payments, delivering goods/services using ICT and ensuring the transfer of property rights of legal entities/individuals to other entities (Pleskach & Zatonatska, 2007).

Based on the Global Digital report authorship of Kemp (2023), 5.44 billion people worldwide use mobile phones, accounting for 68% of the global population. Additionally, there are 5.16 billion Internet users, representing 64.4% of the world population. The number of Internet users increased by 1.9% over the year. Despite challenges such as Russia's aggression against Ukraine leading to high inflation rates and geopolitical instability, the report indicates a growth in e-commerce in Europe. The turnover in European B2C e-commerce rose from €849bn in 2021 to €899bn in 2022, with growth rate decreasing from 12% to 6%. However, the forecast for 2023 suggests a slight increase in growth rate to 8%, indicating a positive trend in European B2C e-commerce turnover (Lone et al., 2023).

In other words, e-commerce has a significant impact on all types of economic activity. For example, in

* Corresponding author. E-mail: *pleskachmarija@gmail.com*

Lithuania percentage of the population accessing the Internet in 2023 amounted to 89%, and percentage of Internet users who bought goods or services online has reached the level of 69%. By comparison, in Latvia and Estonia, percentage of the population accessing the Internet in 2023 of both countries amounted to 92%, and percentage of Internet users who bought goods or services online – 69% та 79% accordingly (Lone et al., 2023). As we can see, *all the Baltic States have demonstrated a steady increase in e-commerce turnover compared to previous years*. For comparison, in Ukraine, despite the war, there is also a tendency to increase the share of digital services in the economy from year to year. For example, the percentage of the population accessing the Internet in 2023 was 81%, and the percentage of Internet users who bought goods or services online reached 73%. In 2022, there were only 57% of online shoppers in Ukraine (Lone et al., 2023). In addition, there is a tendency of wider sales of e-commerce services for export from Ukraine, to the EU and the Baltic States, in particular (Symonenko, 2023).

Such a significant growth of e-commerce and other digital services is impossible without collecting personal data about consumers, their preferences and needs. For example, e-commerce entities such as online retailers need detailed information about existing and potential customers to conduct marketing activities, set up targeted advertising, or sell goods and services. The current problem is that in today's highly competitive environment, information about consumers may be collected in violation of current personal data protection laws, and various digital services may pose a hidden threat to human rights. There are many examples of illegal collection and use of personal data. For example, as Hollister (2019) notes, Google contractors were found to have fraudulently collected biometric data from homeless people and students to improve the Pixel 4 smartphone's facial recognition system. In exchange for face scanning, contractors offered $5 certificates to Starbucks. About another notorious example of the illegal use of people's personal data points out Confessore (2018). It is about the Facebook and Cambridge Analytica data leak (the illegal use of personal data of about 50 million Facebook users by the British company Cambridge Analytica with the assistance of the American company Facebook).

Therefore, given such factors as the steady increase in the number of digital services, electronic applications and online stores, the cross-border nature of e-commerce and the significant deepening of cooperation between Ukraine and the Baltic States, with a focus on strengthening trade and diplomatic relations, *it is an urgent task* to analyze the level of personal data protection in the field of e-commerce in the Baltic States and Ukraine. It is also important to find ways to improve the legal acts regulating this area, provide specific recommendations to consumers of digital services on the protection of their personal data, *in order for* businesses to gain better access to the European digital market, combined with strengthening consumer protection on the Internet in all the jurisdictions under study. For this research was used various *methods of data selection and analysis*. The selected documents related to this article can be divided into 3 main groups: EU law, legal acts of the Baltic States and Ukraine on the protection of personal data in the field of electronic commerce; articles, scientific works; statistical information with annual reports of independent public personal data protection authorities in all the studied countries.

2. The research results

2.1. General overview of the legislation on the protection of personal data in the field of electronic commerce in EU and Baltic States (Lithuania, Latvia, Estonia)

Before we take a closer look at the legal standards of personal data protection in the Baltic States, we should note that Lithuania, Latvia, and Estonia are members of the European Union (EU). This means that these countries are subject to EU law. *The peculiarity of the EU law is that it:*

- firstly, it has direct effect, as its provisions establish subjective rights and obligations directly for individuals and legal entities;
- secondly, it has supremacy over the national law of the Member States. The supremacy of EU law means that its sources have greater legal force than the sources of law adopted within individual member states.

Thus, the activities of business entities in the field of e-commerce in the Baltic States must comply with the requirements of both EU law and national legislation. Given the significant number of possible threats to the privacy of a person as a personal data subject, it is most appropriate to study the EU legislation on personal data protection in e-commerce.

Currently, the key act of the EU regulating e-commerce is *Directive 2000/31/EC* (The European Parliament & the Council of the European Union, 2000).

In accordance with the adopted Strategy for the Development of the Digital Market in the EU, additional measures were taken to harmonize the provisions of European legislation for the further development of e-commerce, including issues related to the protection of personal data of e-commerce consumers, namely:

- consumer protection rules in the field of e-commerce were updated (Directive 2019/2161/EU amended Directive 98/6/EC, Directive 2005/29/EC, Directive 2011/83/EU14) (The European Parliament and the Council of the European Union, 2019b; 1998; 2005; 2011);
- the Directive on contracts for the supply of digital content and digital services (Directive 2019/770/EU15, The European Parliament and the Council of the European Union, 2019a) was adopted. Directive 2019/770/EU on certain aspects relating to contracts

for the supply of digital content and digital services is part of the Digital Single Market Strategy for Europe and, among other things, establishes the seller's obligation to comply with the requirements for the protection of consumers' personal data, including after the termination of the contract.

Examples of services that fall under Directive 2000/31/EC are: online information services; online sales of products and services; online advertising; professional services; entertainment services and basic intermediary services, which may be offered at free to the user and funded through advertising.

At the same time, the main legislative act of the EU in the field of personal data protection (which also applies to the field of e-commerce) is *the General Data Protection Regulation/Regulation (EU) 2016/679 (GDPR)*. This is a regulation within the framework of the EU legislation on the protection of personal data of all individuals within the European Union and the European Economic Area. The GDPR is intended primarily to give citizens and residents of the EU control over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU (The European Parliament & the Council of the European Union, 2016).

The adoption of the GDPR modernized the European Union's personal data protection legislation, which is now able to ensure the protection of fundamental rights in the context of the economic and social challenges of the digital era. The GDPR has established obligations that require organizations *to ensure that their systems automatically apply personal data protection by default*; appoint a data protection officer under certain conditions; comply with data transfer laws; and adhere to the principle of accountability. Under EU law, the regulations are directly applicable and do not require transposition into national law. The GDPR contains comprehensive rules on territorial applicability. It applies to businesses established in the EU, as well as to controllers and processors that are not established in the EU but that provide goods or services to or monitor the behavior of data subjects in the EU.

Another important step towards strengthening the protection of personal data of digital service users was the entry into force on January 1, 2024 of the Digital Services Act (DSA) and the Digital Market Act (DMA), a single set of rules for the entire EU, which aims to create a safer digital space where the fundamental rights of all digital service users will be protected. The Digital Services Act, among other things, is designed to: protect minors on the Internet by prohibiting platforms from using targeted advertising based on the use of personal data of minors; and imposes certain restrictions on advertising and the use of sensitive personal data for targeted advertising, including gender, race and religion (Lekatis, 2023). The Digital Services Act (DSA) proposed by the Commission is based on Directive 2000/31/EC and aims to address new challenges online.

Below, *we will take a closer look at the peculiarities of national legislation on personal data protection in the field of e-commerce in the Baltic States.*

Lithuania

The GDPR is supplemented by Law № XIII-1426 of 30 June 2018 amending Law № I-1374 ("Personal Data Protection Law") (Lietuvos Respublikos Seimas, 2016).

Main Lithuanian' regulator for data protection in sphere of e-commerce is State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija, n.d.).

In addition to the responsibilities outlined in the Article 57 of the GDPR, as stated in the Article 11 of the Personal Data Protection Law, the VDAI is tasked with advising data subjects, data controllers, and data processors on protecting personal data and privacy. It also develops methodological recommendations for personal data protection and makes them publicly accessible on its website. Furthermore, the VDAI is involved in national policy development and implementation related personal data protection. To carry out these duties, the VDAI is granted powers beyond those specified in the Article 58 of the GDPR, as detailed in the Article 12 of the Personal Data Protection Law. For example, these powers include the authority to request information, including document copies, from data controllers, processors, legal entities etc., to fulfil its functions (Buciute, 2024).

Latvia

The GDPR in Latvia is supplemented by Personal Data Processing Law of 21 June 2018 and it came into effect on July 5, 2018 (The Parliament of the Republic of Latvia (Saeima) (2018). Along with the Law is valid the Government Regulations № 620 the Data Protection Specialist Qualification Rules, which were adopted on October 6, 2020. In addition, Government Regulations № 488 Licensing Requirements for the Code of Conduct Monitoring Body entered into force on January 2, 2023, and related Accreditation Requirements for the Code of Conduct Monitoring Body.

According to Latvian law, the GDPR applies beyond EU borders. Even organizations not based in the EU must comply with GDPR if they handle personal data of individuals within the EU for purposes related to offering goods or services or monitoring their behavior within the EU.

Main Latvian' regulator for data protection in sphere of e-commerce is Data State Inspectorate Republic of Latvia (DVI) (2024).

The Data State Inspectorate has implemented various guidelines concerning the GDPR, particularly within the realm of e-commerce. These include:

- Guidance on the Processing of Personal Data for Telemarketing Purposes;
- Guidelines on the Personal Data Processing in the Telemarketing Industry as a Data Processor;
- Guidance on Cookies Placement on Webpages;

– Recommendations on the right to publish information containing personal data in the media and on social networks;
– Guidelines on the processing of personal data when making electronic payments;
– Guidelines on the processing of personal data for commercial purposes.

The DVI, in addition to the tasks outlined in the Article 57 of the GDPR, has various responsibilities as per Section 4 of the Law. These include overseeing data processing compliance with relevant laws, enhancing data protection efficiency, managing the data protection certification process, verifying DPO qualifications, providing recommendations to legislative bodies, assessing data processing systems in public institutions, collaborating with foreign supervisory authorities, and conducting research and analysis within its jurisdiction. Additionally, the DVI ensures transparency, handles information requests from data subjects, and fulfills obligations specified in other legislation (Burkevics, 2023).

Estonia

Data protection in Estonia is mainly regulated by the GDPR, which has been incorporated into Estonian legislation through the Personal Data Protection Act 2018 (PDPA) that became effective on January 15, 2019. (The Parliament of the Estonia (Riigikogu), 2018).

Main Estonian' regulator for data protection in sphere of e-commerce is Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) (2024). As in Latvia, Estonian' regulator for data protection has adopted a number of guidelines in relation to the GDPR, including the sphere of e-commerce. For example:

– Guide to the publication of payment irregularities;
– Reminder for social networking users.

The Estonian Data Protection Inspectorate, in addition to GDPR powers, can: raise public awareness on data risks and rights, provide data subjects with information and cooperate with EU authorities, initiate penalties for non-compliance, collaborate internationally, monitor tech developments, advise on data processing, participate in the European Data Protection Board (EDPB), enforce laws, provide opinions to relevant bodies, and fulfill other legal duties.

The DPI, as per §56(3) of the Personal Data Protection Act, also can: warn controllers and processors of potential PDPA violations; request data collection, deletion, or processing restrictions; order data processing termination, including data destruction or archiving; implement security measures to safeguard personal data if needed, following the specified procedure, except for state agency data processing (Kukk, 2024).

2.2. General overview of the legislation on the protection of personal data in the field of electronic commerce in Ukraine

The current legal framework for the protection of personal data in the field of e-commerce in Ukraine has its own specifics and is somewhat different from the norms that operate in the EU. *This is due to several factors:*

– firstly, Ukraine is on the way to full EU membership, and therefore national legislation still needs to be harmonized with the European one;
– secondly, there is a certain lag between legislative work and technological development in Ukraine.

Today, the main law that defines the organizational and legal framework for e-commerce in Ukraine, establishes the procedure for electronic transactions using information and communication systems, and defines the rights and obligations of participants in e-commerce relations is the Law of Ukraine "On Electronic Commerce" (The Ukrainian Parliament (Verkhovna Rada of Ukraine), 2015). Part 2 of Article 8 of this Law regulates the legal status of the buyer, obliges the buyer who accepts the offer of the other party to enter into an electronic contract to provide the information necessary for its conclusion. *What kind of information are we talking about?* Part 6 of Article 8 of this Law of Ukraine contains the following blanket provision: "*The list of information required for the execution of an electronic transaction is determined by the legislation of Ukraine or by agreement of the parties*". Therefore, each online store in Ukraine decides for itself what kind of information can be required from the buyer, and it becomes an "agreement of the parties" when the buyer agrees to the terms and conditions proposed by the seller (Porytko, 2017). In this case, the Law of Ukraine "On Personal Data Protection" (The Ukrainian Parliament (Verkhovna Rada of Ukraine) (2010) is the legal guideline that details what information should be collected about the buyer and in what way. This Law regulates legal relations related to the protection and processing of personal data and is aimed at protecting the fundamental rights and freedoms of persons. Currently, there is an urgent need in Ukraine to clarify the provisions of the legislation on consent to data processing and to increase the liability of online resources for violations. This is primarily due to the fact that under the EU-Ukraine Association Agreement, Ukraine has undertaken to bring its national legislation in line with the requirements of EU legislation, including the GDPR. *A number of steps have been taken in this direction*, for example, in 2018, the Parliament of Ukraine announced consideration of *the draft updated Law of Ukraine "On Personal Data Protection" (*The Ukrainian Parliament (Verkhovna Rada of Ukraine), 2018). However, as of 2024, this draft law has not been adopted.

At first glance, it may seem that the GDPR does not apply in Ukraine, but this is not the case. There are territorial and subject-specific peculiarities of its application in Ukraine. *That is, there are cases when Ukrainian companies (regardless of the country of incorporation/conduct of their main activities) may also be subject to the GDPR. For example:*

– the e-commerce entity is focused on the EU market (the target audience is people living in the EU (GDPR rules are not tied to citizenship);

– the e-commerce entity has an office/representative office (for example) in the EU, EEA;
– the e-commerce entity has a foreign domain;
– prices on the website are indicated in foreign currency;
– the e-commerce entity sells goods (services) and offers their delivery to the EU (Riabets, 2023).

Unlike the Baltic countries, which have already established independent public bodies for personal data protection, the specificity of the Ukrainian model is that there is no separate regulatory body in the field of personal data protection (including e-commerce). At present, *the Ukrainian Parliament Commissioner for Human Rights (Ombudsman) is responsible for compliance with the legislation in this area* (The Ukrainian Parliament Commissioner for Human Rights, 2024).

Under the Law of Ukraine "On Personal Data Protection", 2010, the Ukrainian Parliament Commissioner for Human Rights (The Commissioner) oversees compliance with personal data protection laws. This includes ensuring that data processing aligns with Ukraine's Constitution, the Law of Ukraine "On Personal Data Protection", and international treaties ratified by Verkhovna Rada (The Ukrainian Parliament (Verkhovna Rada of Ukraine), 2010). The Commissioner conducts inspections of various entities verify compliance, with inspections being scheduled or unscheduled, on-site or off-site. The procedure for these inspections is outlined in the Commissioner's approved guidelines. Disputes regarding personal data protection can also be resolved through court appeals to determine the legality of data dissemination (Martynenko, 2021).

3. Comparative analysis of the legislation on the protection of personal data in the field of electronic commerce between the Baltic States (Lithuania, Latvia, Estonia) and Ukraina

Due to the materials of the previous sub-sections of this study, we will compare the requirements of the Ukrainian current and prospective legislation, as well as the legislation of the Baltic States on the protection of personal data in e-commerce (based on the *following criteria):*

3.1. The scope of the law (personal, territorial, material scope)

There are no national law variations in Baltic States, GDPR provisions shall be applied.

The scope of the GDPR, as well as all national laws of the Baltic States in terms of the range of persons, concerns the protection of personal data of individuals.

According to the GDPR subject matter applies to legal relations related to the protection and processing of personal data, but specifies a list of relations that are not covered by the GDPR (for example, activities that go beyond the scope of EU law).

With regard to the territorial criterion, the GDPR applies to:

– processing of personal data by a controller or operator registered in the EU;
– processing of personal data by a controller or processor registered outside the EU, but processing data of individuals located in the EU.

Current Law of Ukraine "On Personal Data Protection" regulates legal relations related to the protection and processing of personal data and is aimed at protecting fundamen tal human rights and freedoms (in terms of the range of persons, it applies to individuals).

In terms of subject matter jurisdiction, this Law applies to legal relations related to the protection and processing of personal data, in particular, to processing carried out in whole or in part with the use of automated or non-automated means.

The Law does not define its territorial effect, but in the cases described in clause 1.2 of this study, the GDPR will take precedence over the Law.

The scope of the ***Prospective Law of Ukraine "On Personal Data Protection" (draft law)*** *coincides with the GDPR.*

3.2. Key definition: "personal data"

There are no variations of the GDPR in Baltic States. "Personal data" under the GDPR is a broad and detailed concept because it is "any information relating to an individual".

According to the Law of Ukraine "On Personal Data Protection", "personal data" means information or a set of information about an individual who is identified or can be specifically identified.

As in the GDPR, the draft law defines "personal data" as any information relating to an identified or identifiable individual.

3.3. Grounds for personal data processing

The GDPR establishes several grounds on which personal data may be legally processed. The main ground is ***the data subjects' consent*** to the processing of his or her personal data. Other grounds include the need to fulfill a contract with the data subject, the need to protect the vital interests of the data subject, the need for the controller to fulfill its duties, etc.

The current legislation in Ukraine regarding personal data protection aligns with the GDPR, outlining similar principles for processing personal data as stated in the Article 11. One of the main principles include obtaining consent from the data subject.

3.4. Responsibility

The GDPR establishes the following general provisions on liability for unlawful processing of personal data:

– 2% of the total annual turnover or €10 million, whichever is higher, for violations of the provisions on the processing of minors, controller's and processor's obligations, etc.; or

– 4% of the total annual turnover or €20 million, whichever is higher, for violations of the provisions on data processing principles, data subjects' rights, data transfers to third countries, etc.

At the same time, the Baltic States have their own specifics of imposing fines on violators.

In Lithuania, administrative fines for infringements can be imposed within two years of the date the violation occurred or, if ongoing, within two years of its committing. The Personal Data Protection Law allows for fines for breaches of the GDPR and the Personal Data Protection Law. Fines can range from up to 0.5% to 1% of an authority's or body's budget, not exceeding €30 000 or €60 000, depending on the severity of the violation. Additionally, fines can be imposed on authorities or another subject engaged in economic activities for violations specified in the GDPR.

In Latvia, violators may be held civilly, administratively or criminally liable depending on the severity of the violation (Burkevics, 2023).

The legal system of Estonia does not allow for administrative fines as set out in the GDPR. The requirements of Article 83(9) of the GDPR have yet to be implemented. In addition to the sanctions provided for in the GDPR, the PDPA establishes sanctions in some cases (Kukk, 2024).

Ukrainian law stipulates that if personal data has been collected and used illegally and the owner of such data has discovered this violation, he or she may request the deletion and prohibition (termination) of personal data processing.

It also provides for the following possible consequences of violations (liability):

– failure to notify (late notification) the Commissioner of personal data processing or change of information – for citizens from UAH 1700 to UAH 3400 and for officials, citizens – business entities from UAH 3400 to UAH 6800;
– failure to notify (late notification) the Commissioner of personal data processing or change of information – for citizens from UAH 3 400 to 5 100 and for officials and citizens – business entities from UAH 3400 to 17 000;
– repeated commission of the above violations (within a year) for individuals from UAH 5100 to UAH 8500 and for officials and citizens who are business entities from UAH 8500 to UAH 34 000;
– failure to comply with the established procedure for the protection of personal data, which led to illegal access to them or violation of the rights of the personal data subject – for individuals from UAH 1700 to 8500 and for officials and citizens – business entities from UAH 5100 to 17 000;
– repeated violation of the above within a year – from UAH 17 000 to UAH 34 000.

It also provides for criminal liability for violation of privacy.

The Draft Law *significantly increases liability for violation of legislation in the field of personal data protection:*

– the smallest fine in the amount of UAH 10 000 to UAH 30 000, for legal entities in the amount of 0.05% to 0.1% of the total annual turnover of such legal entity, but not less than UAH 30 000 for each individual violation;
– the largest fine – in the amount of UAH 100 000 to UAH 300 000, for legal entities in the amount of 3% to 5% of the total annual turnover of such legal entity, but not less than UAH 300 000 for each individual violation.

In addition, the Draft Law provides for a provision according to which bringing the perpetrators to liability under this Draft Law, as well as administrative or criminal liability does not deprive the subjects of personal data, the right to compensation for material and non-pecuniary damage caused by the violation of their rights in the manner prescribed by civil legislation.

3.5. Responsible authority (Controlling authority)

All the Baltic States have already established independent public authorities for personal data protection. In Lithuania – State Data Protection Inspectorate; in Latvia – Data State Inspectorate Republic of Latvia; in Estonia – Estonian Data Protection Inspectorate.

Ukraine does not have a separate regulatory body in the field of personal data protection (including e-commerce). The Ukrainian Parliament Commissioner for Human Rights is in charge of these issues, 2010.

The draft law provides for the establishment of an independent executive body with a special status to implement international standards in the field of protection of the right to access information and the right to personal data protection at the national level. In particular, *the National Commission on Personal Data Protection and Access to Public Information should become such a body*.

3.6. Statistics on violations of personal data protection legislation in the field of e-commerce

Lithuania

In accordance to the Annual report of State Data Protection Inspectorate, statistically, *breaches of confidentiality prevail in Lithuania.* In 2023, they comprised as much as 76% of all cases; 10% of cases were attributed to integrity breaches; 10% of cases – to accessibility breaches; and in 4% of cases, the breach incident was not deemed to be the personal data breaches In Lithuania, the largest fine issued was €110 000 and the total value of all fines was €244 500. In 2019, the value was €61 000, while by 2021 that sum had risen to €160 000. A total of 57 fines had been issued by 2022. Lastly, from May 2018 to December 2022, 953 personal data breaches were reported, of which 258 were reported from January 2022 to December 2022 (State Data Protection Inspectorate (VDAI), 2024).

Latvia

In 2022 and 2023 *telemarketing service providers and recipients of their services* have been in focus of the Data State Inspectorate Republic of Latvia preventive inspections.

According to the annual report of the Data State Inspectorate of the Republic of Latvia for 2022, the supervisory authority received 708 complaints, 191 of which concerned the processing of personal data on social networks and other Internet sites. In addition, the report indicates that the Data State Inspectorate of the Republic of Latvia applied enforcement measures (i.e., warnings, instructions, reprimands, and process restrictions) in 234 cases, while it issued 16 decisions on administrative offenses, and in 12 of these 16 cases, the Data State Inspectorate of the Republic of Latvia imposed fines ranging from €200 to €1.2 million. In total, in 2022, the Data State Inspectorate of the Republic of Latvia imposed fines totaling €1 223 059 (Data State Inspectorate Republic of Latvia, 2023).

Estonia

Estonia is among the countries in the EU with the *lowest GDPR fines applied*. This is partly due to the unique nature of procedural rules. Namely, in Estonia, fines are applied only in misdemeanor proceedings. The largest GDPR fine issued in Estonia was only €280, while the largest enforced non-compliance levy was €10 000 (Ojala et al., 2023).

Ukraine

According to the annual report of the Ukrainian Parliament Commissioner for Human Rights (2023), published on April 5, 2023, during the reporting period, the Commissioner received 8027 appeals (including those related to issues of illegal processing of personal data – 3%, the right to access information about oneself – 2%, organization of personal data processing – 1% and recommendations and clarifications on the practical application of personal data protection legislation – 1%).

In 2022, the Commissioner recorded *the following violations of the legislation on personal data protection personal data:* unlawful processing of personal data, in particular their unlawful dissemination and use, failure to provide the personal data subject with complete information about the owner of personal data, improper execution of consent to the processing of personal data personal data, failure to provide access to their personal data (information about themselves).

As in previous years, violations regarding the unlawful processing of personal data continue to be a key problem in this area, although the number of reports in compared to 2021 has significantly decreased. In 2022, 844 appeals were received and cases of human and civil rights violations were responded to:

– 60% of reports related to the illegal processing of personal data;
– 28% of reports of violations of the right to access information about oneself;
– 12% of reports concerning the organization of personal data processing (the vast majority of them concerned improper processing of personal data by e-commerce entities: Internet pharmacies, shops, etc.).

The Commissioner opened 66 proceedings on these notifications, which resulted in response measures to restore the rights of citizens (personal data subjects).

Unfortunately, the annual report does not provide an opportunity to track the financial component of the imposed penalties and the effectiveness of their implementation (The Ukrainian Parliament Commissioner for Human Rights, 2023).

4. Conclusions and recommendations

1. Lithuanian, Latvian, Estonian and Ukrainian approaches to personal data protection in the field of e-commerce are similar in many ways, yet different at the same time. There are several reasons that have led to the features in their legal models. Given that all three Baltic countries are EU members, they are subject to the EU's unified personal data protection legislation (including in e-commerce). *As we can see:*

– all three countries have fully implemented the GDPR at the level of national laws, without their own personal, territorial, material scope. At the same time, Latvia, among the three countries, has the largest array of bylaws that detail or clarify how to apply the GDPR in a particular area;
– all Baltic countries have the same approach to understanding the basic terminology in this area, as well as the grounds for processing personal data;
– Lithuania, Latvia, and Estonia have their own independent public personal data protection authorities (which are also responsible for personal data protection in e-commerce);
– another common feature of these countries is the general tendency to increase liability for violations of legislation in this area. This is primarily due to the fact that all Baltic countries demonstrate a steady increase in e-commerce turnover from year to year, which is impossible without collecting personal data about consumers, their preferences and needs.

Given Ukraine's aspirations to become a full-fledged member of the EU, some of the GDPR requirements have already been implemented in *Ukrainian laws to varying degrees*. For example, the subject matter and subjective effect of the Law of Ukraine "On Personal Data Protection" is identical to that enshrined in the laws of the EU and the Baltic States. The grounds for processing personal data are the same for Ukraine as well as for Lithuania, Latvia, and Estonia, the main one being *the consent of the personal data subject* to the processing of personal data.

2. Despite the common focus of national legislation on strengthening liability for the illegal processing of personal data in e-commerce, *each of the Baltic States*

has its own specifics in the procedures for bringing to liability and determining the amount of fines imposed. These differences also entail differences in the effectiveness of national legal mechanisms, which is proved by the statistics presented in the annual reports of the supervisory authorities. For example, *Latvia* has the highest total amount of fines among the Baltic countries, *Lithuania* has the highest number of personal data violations, and *Estonia* has the lowest value of fines in the Baltics. At the same time, the low statistics of administrative fines is not due to the absence of violations. One of the reasons is the lack of resources in the Estonian Data Protection Inspectorate, which has become so serious that it leads to delays in responding to requests (Hübner, 2021). *Statistics show that the Baltic States still have problems with personal data protection, including in the field of e-commerce*. However, the effective protection introduced by the GDPR and the implementation of the recommendations should lead to a significant reduction in the number of complaints and fines in this area in the future.

Ukrainian practice in this area is characterized by a much smaller number of cases and fines, not due to the absence of violations, but due to the low legal culture of citizens regarding their personal data and the imperfection of the current legislation. Ukraine, despite the exhausting war with Russia, has taken many steps towards modernizing its data protection legislation. In particular, in 2022, *the Ukrainian Parliament adopted a number of amendments to the current legislation governing personal data protection,* including the Law of Ukraine "On Personal Data Protection" regarding cloud services, processing of personal data during martial law, provision of medical services and statistical activities. A new draft Law of Ukraine "On Personal Data Protection" is scheduled for consideration in 2024, as well as the establishment of an independent regulatory authority with the implementation of the standards set forth in the GDPR into Ukrainian national legislation. It is expected that the maximum regulatory approximation of personal data protection in the field of e-commerce to the harmonized EU rules will lead to a reduction of obstacles and restrictions in multilateral trade between Ukraine, the EU and the Baltic States, in particular. As a result, businesses will have better access to each other's markets, which, combined with stronger consumer protection and increased transparency in e-commerce, will lead to an increase in e-commerce and have a positive effect on the economies of the Baltic States and Ukraine.

3. *The following key comprehensive recommendations follow from this research. Personal data subjects (e-commerce entities of all countries) that process personal data should be:*

– adhere to the principles of personal data protection and liability provided for by the GDPR (legality, fairness and transparency; limitation of the purpose of use (use data only for the purpose about which the user was informed, data minimization (do not collect more data about the user than is necessary for work); accuracy (accurate and up-to-date data should be stored), storage limitation (collected data can be stored only for the time necessary to achieve the purpose for which it was collected, confidentiality, liability (presumption of guilt – the one who processes personal data must prove that you comply with all the principles of the GDPR);
– comply with the general requirements to be considered an e-commerce entity that properly handles customers' personal data.

These requirements include:

– a link to the data protection policy (Regulation on the Processing and Protection of Personal Data) on the website, which is developed in accordance with the GDPR rules. Such policy should contain the following indicative parts (chapters): general concepts and scope of application of the regulation; the list of personal data bases controller and processor by the subject of e-commerce; purpose of personal data processing; procedure for processing personal data; the location of the personal database; conditions for disclosing information about personal data to third parties; protection of personal data; rights of the subject of personal data; the procedure for handling requests of the subject of personal data;
– the data protection policy must contain a clear purpose of processing personal data in the online store and its scope. An e-commerce company cannot ask customers to consent to "any action" with their data. In general, the GDPR prohibits the use and demand of personal data for purposes other than the execution of an electronic transaction. That is, we are talking about the implementation of the "Data Minimization" principle. That is, "by default" the online store must request a minimum set of data about the client, which is allowed to be collected and processed only for the purpose of payment and delivery of goods to the client's address. Obviously, the client is interested in providing as few information about himself as possible. However, the exception will be the situation if the buyer makes a purchase anonymously;
– the website must contain a special box that the user must tick to confirm that person has read the data protection policy before submitting person's information. Such box should become available to the user no earlier than after the amount of time that is really necessary for reading; and a special box that the user must tick to confirm the purchase if it is necessary to provide personal information (informed consent).

The consent of an individual for the processing of their personal data is a voluntary expression of their intention, given that they are adequately informed, to authorize the processing of their personal data for a specific purpose, either in written form or in a manner that clearly indicates consent. In the realm of e-commerce, the individual's consent for personal data processing can

be obtained during website registration by selecting the option to consent to the processing of their personal data for the specified purpose, ensuring that the system does not initiate any data processing until consent is provided. That is, the user's consent must be: voluntary, clear, informed; requests for consent must be clearly visible and written in plain language; the user has the right to withdraw consent to the processing of his data at any time, as well as exercise the right to be forgotten; children under the age of 13 can give consent only with the permission of their parents; the online store must keep documentary evidence of consent to data processing:

- availability of information about the use of cookies and the specifics of such use;
- compliance with cybersecurity standards. Cyber security of an online store is a complex multi-level system consisting of many components. Here are just a few examples: security of payment systems (it is important to ensure that financial data is protected from theft, fraud or abuse. Financial security of credit cards means the use of security technologies such as chips and PIN codes, data encryption during online transactions, such as 3D Secure, cardholder authentication (CVV/CVC codes), as well as control of card transactions (SMS or push notifications), etc.;
- availability of clear, accessible and transparent information about the ways in which users can contact representatives of the online store to learn more about the contractual and legal aspects of the products and services offered on it. *A separate area of activity to improve the level of protection of personal data in the field of e-commerce* should be monitoring inspections of the state of human rights observance, as well as explanatory, educational and rulemaking work by the entities responsible for the protection of personal data in the field of e-commerce in each of the studied jurisdictions.

Acknowledgements

The author would like to thank the Lithuanian Scientific Council (Lietuvos mokslo taryba) for their financial support in this research and Mykolas Romeris University represented by Dovilė Sagatienė and Vaidas Jurkevičius who provided advice and support during the writing of this publication.

Funding

This work was supported by the Lithuanian Scientific Council (Lietuvos mokslo taryba) [grant number P-PD-23-170].

Disclosure statement

The author does not have any competing financial, professional, or personal interests from other parties. The author is no competing interests to declare.

References

Buciute, R. (2023). Lithuania – Data protection overview. https://www.dataguidance.com/notes/lithuania-data-protection-overview

Burkevics, A. (2023). *Latvia – Data protection overview*. https://www.dataguidance.com/notes/latvia-data-protection-overview

Confessore, N. (2018, April 4). Cambridge analytica and Facebook: The scandal and the fallout so far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Data State Inspectorate Republic of Latvia [DVI]. (2023). https://www.vdi.gov.lv/lv/parskati?utm_source=https%3A%2F%2Fwww.google.com%2F

Data State Inspectorate Republic of Latvia [DVI]. (2024). https://www.dvi.gov.lv/en

Republic of Estonia Data Protection Inspectorate (Andmekaitse Inspektsioon). (n.d.) https://www.aki.ee/en

Hollister, S. (2019). *Google contractors reportedly targeted homeless people for Pixel 4 facial recognition*. https://www.theverge.com/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition

Hübner, R. (2021). *In a nutshell: Data protection, privacy and cybersecurity in Estonia*. https://www.lexology.com/library/detail.aspx?g=58b92eec-bc19-4e37-b79c-3cbe72fc5fca

Kemp, S. (2023). *Digital 2023: Global overview report*. https://datareportal.com/reports/digital-2023-global-overview-report

Kukk, U. (2024). *Estonia – Data protection overview*. https://www.dataguidance.com/notes/estonia-data-protection-overview

Lekatis, G. (2023). *The Digital Services Act (DSA) – Regulation (EU) 2022/2065*. https://www.eu-digital-services-act.com-/?fbclid=IwAR1Aqf_8M03cRUB8BtIU5nMZmFcPut_6gvj12GhoGuNqlEqgkd5Pm0fl8yE

Lietuvos Respublikos Seimas. (2016). *Republic of Lithuania Law on Legal Protection of Personal Data* (Last amended 2016, November 3, No. I-1374). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae

Lone, S., Weltevreden, J., & Luharuwala, A. (2023). *European e-commerce report* (p. 2, 3, 36, 42, 43, 82). Amsterdam University of Applied Sciences & Ecommerce Europe. https://ecommerce-europe.eu/wp-content/uploads/2023/11/European-Ecommerce-Report-2023-Light-Version.pdf

Martynenko, O. (2021). *Analysis of the draft Law of Ukraine "On the National Commission for the Protection of Personal Data and Access to Public Information"* (2021, October 18, No. 6177). https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-natsionalnu-komisiiu-z-pytan-zakhystu-personalnykh-danykh-ta-dostupu-do-publichnoi-informatsii-6177/

Ojala, S. V., Kuuskmaa, L. M., Matulytė, R., & Terjuhana, J. (2023). *Statistics on GDPR fines issued and data breaches reported in the Baltics*. https://www.sorainen.com/publications/statistics-on-gdpr-fines-issued-and-data-breaches-reported-in-the-baltics/

Pleskach, V., & Zatonatska, T. (2007). E-commerce. In *Elektronna komertsiya: Pidruch.* [Electronic commerce: tuto- rial] (pp. 55). Kyiv: Znannia.

Porytko, A. (2017). *Protection of personal data in the online-shop*. https://online.dtkt.ua/2017/13/48089

Riabets, J. (2023). Why it is important for businesses to protect personal data of customers. https://www.juscutum.com/news/chomu-biznesu-vazhlivo-zahishchati-personalni-dani-kliientiv

State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija, VDAI). (n.d.). https://vdai.lrv.lt/en/

State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija, VDAI). (2024). *Personal data breaches in Lithuania during the year of 2023*. https://vdai.lrv.lt/en/news/personal-data-breaches-in-lithuania-during-the-year-of-2023/

Symonenko, K. (2023). *Logistics and e-commerce news: New post office in all Baltic countries, Rozetka connects Shafa.ua, food delivery service from Uklon and much more*. https://rau.ua/novyni/novini-kompanij/novini-e-commerce-10-23/

The European Parliament and the Council of the European Union. (2019a). *Directive 2019/770/EU15 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services* (2019, May 20, No. 32019L0770). Official Journal of the European Union, L136/1. https://eur-lex.europa.eu/eli/dir/2019/770/oj

The European Parliament & the Council of the European Union. (2019b). *Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules* (2019, November 27, No. 32019L2161). Official Journal of the European Union, L 328/7. https://eur-lex.europa.eu/eli/dir/2019/2161/oj

The European Parliament & the Council of the European Union. (2016). *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)* (2016, April 27, No. 32016R0679). Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

The European Parliament and the Council of the European Union. (2011). *Directive 2011/83/EU14 of the European Parliament and of the Council*. https://www.legislation.gov.uk/eudr/2011/83/body

The European Parliament and the Council of the European Union. (2005). *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')* (2005, May 11, No. 32005L0029). Official Journal of the European Union, L149/22. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029

The European Parliament, & the Council of the European Union. (2000). *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')* (2000, June 8, No. 32000L0031).https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

The European Parliament and the Council of the European Union. (1998). *Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers* (1998, February 16, No. 31998L0006). Official Journal of the European Communities, L80/27. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0006

The Parliament of the Estonia (Riigikogu). (2018). *Isikuandmete kaitse seadus* [Personal Data Protection Act] (2018, December 12, No. 367). https://www.riigiteataja.ee/akt/104012019011

The Parliament of the Republic of Latvia (Saeima). (2018). *Personal Data Proceesing Law* [Fizisko personu datu apstrādes likums]. https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law

The Ukrainian Parliament (Verkhovna Rada of Ukraine). (2010). *About the Protection of Personal Data. Law of Ukraine.* [Pro zahyst personalnyh danyh]. https://zakon.rada.gov.ua/laws/show/2297-17#Text

The Ukrainian Parliament (Verkhovna Rada of Ukraine). (2015). *About E-commerce Law* [Pro elektronny komerciu]. https://zakon.rada.gov.ua/laws/show/675-19#Text

The Ukrainian Parliament (Verkhovna Rada of Ukraine). (2018). *The draft Law of Ukraine "On Personal Data Protection"* [Proekt zakony Pro zahyst personalnyh danyh]. https://www.kmu.gov.ua/bills/proekt-zakonu-pro-zakhist-personalnikh-danikh

The Ukrainian Parliament Commissioner for Human Rights [Ombudsman]. (2024). https://ombudsman.gov.ua/

The Ukrainian Parliament Commissioner for Human Rights [Ombudsman]. (2023). *Annual report on the state of observance and protection of human and citizen rights and freedoms in Ukraine in 2022*. https://ombudsman.gov.ua/report-2022/