Review Article

UDC: 342.738(497.11)
338.482:34
doi: 10.5937/menhottur2301193L

Protection of personal data in the tourism sector

Sonja Lučić[1*]

[1] University of Kragujevac, Faculty of Law, Kragujevac, Serbia

Abstract: This research aims to explain certain aspects of the complex legal system of personal data protection. The paper is based on the analysis of domestic and EU regulations that regulate the rights of citizens to the protection of personal data. The paper provides an overview of the obligations that must be fulfilled by tourism entities in order to ensure that the processing of personal data is carried out in accordance with the law. In addition, the risks associated with the processing of personal data and the possibility to ensure the security of data processed by providers of tourist services are listed. The research showed that there are many open questions in the tourism sector regarding the implementation of regulations on the protection of personal data.

Keywords: personal data, individuals, protection, tourism
JEL classification: K10, Z30

Zaštita podataka o ličnosti u turističkom sektoru

Sažetak: Ovo istraživanje ima za cilj da objasni pojedine aspekte složenog pravnog sistema zaštite podataka o ličnosti. Rad se zasniva na analizi propisa koji na evropskom i nacionalnom planu regulišu prava građana na zaštitu ličnih podataka. U radu je dat pregled obaveza koje treba da ispune turistički subjekti kako bi se osiguralo da se obrada podataka fizičkih lica vrši u skladu sa zakonom. Osim toga, navedeni su i rizici povezani sa obradom ličnih podataka i mogućnosti da se obezbedi bezbednost podataka koje obrađuju pružaoci turističkih usluga. Istraživanje je pokazalo da u turističkom sektoru ima dosta otvorenih pitanja u vezi sa implementacijom propisa o zaštiti ličnih podataka.

Ključne reči: podaci o ličnosti, fizička lica, zaštita, turizam
JEL klasifikacija: K10, Z30

1. Introduction

One of the consequences of information technologies development in the last twenty years is the increase in the importance of information and data. Technological advances have made it possible to digitally collect vast amounts of data and then transmit, process, and transmit it across a global network. Businesses of companies are increasingly focused on adapting their products and services to the needs of consumers and using information from and about

* slucic@jura.kg.ac.rs

potential and existing consumers for this purpose. In the course of technological progress, there is a constant transfer of data in social life. After an online purchase or online reservation of services, the system remembers information and data transfer. Based on these data, similar products or services can be recommended to the user and the company can increase its sales or service provision. Data processing is therefore an important success factor, especially in business. The term "processing" includes, among other things, the collection, storage, modification, deletion, dissemination, disclosure through transmission and use of personal data (Chatzopoulou, 2021, p. 125).

The transmission and automatic processing of data have their downsides. If the data is further processed without protection, the information may be freely available to third parties. In this way, misuse of data can easily occur. Given that globalization and related social changes lead to strong networking, it is important to protect data. Data protection generally refers to regulations aimed at protecting personal data and preventing misuse of data by third parties. Since many areas of society are affected, there are different data protection principles.

Defining the concept of data and protection of personal data is not an easy task. Different meanings are used for these terms today. Data protection means the protection of information that is not intended for the general public. Personal data contains information that directly or indirectly relates to a natural person. In this sense, personal information is, for example, first and last name, nickname, e-mail address, citizenship, data from a passport or identity card, travel visas, and data from a health record. However, data protection is not only limited to the protection of personal data. It also includes the protection of an individual's freedom to decide for himself what will happen to his data and when it can be processed. On the one hand, data protection protects citizens from misuse of their personal data. On the other hand, it includes the right of citizens to informational self-determination.

Information self-determination is a topic that is becoming increasingly important in the age of digitization and information technologies. Informational self-determination contains two rights: the right of every person to disclose information about himself and the right to freely decide not to disclose it. In addition, every person has the right to decide what will happen to their data and what it should not be used for. Although the right to informational self-determination is not yet explicitly established by the constitutions of most countries, including ours, according to judicial practice, it represents a basic right to data protection and an expression of the general right to personality. The judgment on the census of the German Federal Constitutional Court was crucial for the establishment of the right to informational self-determination (Judgment of the First Senate of 15 December 1983 - 1 BvR 209/83). The reason for this judgment was the census planned in the first half of 1983 in the Federal Republic of Germany. The State wanted to collect a lot of personal data in the census under the "Census Act", including detailed information about family and civil partnerships, housing situation, educational and vocational training and employment, professional status, working hours and commute. Several constitutional appeals were filed against the planned census, which ultimately led to the so-called census verdict. In this, not only the illegality of the planned census was determined, but also the law on the census was declared unconstitutional. Referring to the general right of personality as a constitutional right, this judgment established the right of citizens to informational self-determination.

Today, a large amount of data is also processed in the tourism sector. Based on the analysis of EU regulations and domestic regulations on the protection of personal data, the following hypotheses were formulated:

H_1: Tourism companies must respect certain principles when processing personal data.
H_2: As a rule, travel companies may not process special categories of personal data.
H_3: Travel companies must respect the rights of natural persons concerning personal data.

2. Materials and methods

2.1. Personal data protection in the European Union

The area of personal data protection at the EU level was first regulated in 1995 (Andonović & Prlja, 2020, p. 119). In the meantime, various external and internal factors, such as the increasing use of the Internet, the development of information and communication technologies, the increasing use of data in business, and significant violations of privacy rights have influenced the need to regulate this area in detail (Andonović & Prlja, 2020, p. 119). In this sense, the General Data Protection Regulation (hereinafter: GDPR) was adopted in the EU on April 27, 2016. This Regulation, which came into force on May 25, 2018, is a far-reaching, uniform and a partially new law on data protection with direct application throughout the EU. This regulation is of great importance, especially with regard to increasingly advanced digitalization as one of the characteristics of the 21st century. Before the entry into force of this Regulation, especially in cross-border traffic, there was legal uncertainty regarding the protection of personal data, both on the side of consumers and on the side of business entities (Feiler & Forgó, 2016, p. 5).

The goal of adopting the General Regulation is to standardize data protection in the EU and thus create the same data protection standards for all member states. In addition to the direct application of the GDPR, member states have the freedom to regulate certain issues, e.g. from which year a minor can effectively consent to the processing of his personal data or whether fines can be imposed on authorities and public bodies (Feiler & Forgó, 2016, p. 6). On the other hand, GDPR does not provide definitive solutions in all areas. Hence, judicial practice, especially of the EU Court of Justice, is of great importance in regulating the protection of personal data in the EU (Fercher & Riedl, 2016, p. 31). However, based on additional information, the Internet provider could identify this visitor. In this case, the identity of the website visitor can at least be determined, which means that the provisions of the GDPR apply to him/her (Feiler & Forgó, 2016, p. 4). For example, when registering on a certain online platform, a natural person does not provide his/her name or any other information, except his/her e-mail address. However, based on this data, that natural person can be identified.

GDPR regulates data protection of natural persons. In other words, legal entities are excluded from the scope of the GDPR, unless the company name, for example, contains the name of a natural person. However, in the tourism industry, companies store the contact details of their partners, which is why the data related to this entry is covered by the GDPR.

The GDPR does not apply to the protection of personal data that is used exclusively for private purposes. These family or private activities include, for example, using social networks exclusively for private purposes (Hladjk, 2016, p. 40). This means that if, for example, an employee of a hotel forms a Viber group for planning joint leisure activities, while the employer does not influence the content or participants of this group, then this form of communication is not covered by the GDPR.

In a territorial sense, the GDPR applies to all processing of personal data within the business activities of entities based in the EU, regardless of whether the processing is carried out in the territory of the EU or outside it (Andonović & Prlja, 2020, p. 122). However, the provisions of the GDPR also apply to data processing carried out by companies based outside the EU but processing personal data of EU citizens, or to companies based outside the EU but with one or more branches in the EU. In this way, the territorial application of the GDPR is largely extended to countries that are not members of the EU, but that have strong

economic cooperation with its market. This includes the Republic of Serbia, which, among other things, has good tourism cooperation with entities on the territory of the EU.

The GDPR protects all personal data, both those processed manually and those processed electronically or through video surveillance.

2.2. Personal data protection in Serbia

Our country recognized in time the need to protect personal data. In 2018, the Personal Data Protection Act (hereinafter PDPA – The Law on Personal Data Protection - Official Gazette of the RS No. 87/2018) was adopted in Serbia, which replaced the previous law that has been in force since 2008. The PDPA regulates the right to protection of natural persons in connection with the processing of personal data, the principles of processing, the rights of persons to whom the data refer, the obligations of the processor of personal data, the transfer of personal data to other countries. The PDPA is largely aligned with the GDPR. However, in relation to the GDPR, our Law does not contain a preamble, foresees milder sanctions, and does not regulate video surveillance issues. The PDPA establishes a personal data protection system regardless of whether it is applied by persons under private or public law. In this sense, the PDPA also obliges tourist subjects, such as, for example, travel agencies, hotels, restaurants, airlines. These entities collect various types of data, such as customers' first and last names, addresses, unique identification number, number passports, nutritional information, medical condition or even religious affiliation (Kędzior & Sadowska, 2019, p. 71). In certain situations, these entities transfer data, for example a travel agency transfers data to a hotel, airline or insurance company.

The obligation to protect personal data also exists within the so-called smart tourism activities (Gretzel et al., 2015, p. 42). Unlike e-tourism, which digitally connects individuals with travel companies, smart tourism is based on the application of artificial intelligence, cloud computing, the Internet of Things (Buhalis, 2020, p. 268). Thanks to these technologies, tourists can experience a better, higher quality and more interactive trip (García et al., 2018, p. 168).

The PDPA does not provide for special regulations relating to certain areas of social life. In other words, the Law does not introduce any special conditions for data processing that would be more or less strict compared to other sectors. In the continuation of the paper, an overview of certain provisions of this law will be given, which are of importance for the obligations of tourism entities with regard to the protection of personal data that they encounter in their work.

3. Implementation of regulations on the protection of personal data in the tourism sector

3.1. Principles of personal data processing

Companies must follow certain principles when processing personal data. Random and unplanned data collection is not allowed. Personal data can only be processed legally, for specific purposes and in a factually correct manner. The volume of data processed should correspond to the purpose of the processing. It is questionable whether online retailers, for example, absolutely need a phone number to be able to process an order. However, this does not apply to companies that provide travel services. After fulfilling the purpose of processing, personal data must be deleted.

Data protection includes technical and organizational measures that the company must implement. Employees must be committed to confidentiality and respect for data protection. When working with personal data, companies must pay special attention to the principles of processing established by law.

The basic principle of personal data processing is the legality of the processing. The PDPA in Art. 12 lists the possible legal bases for processing personal data. The first and most common legal basis for processing personal data is the consent of the natural person, i.e. data subject. Consent can be given in writing or electronically by clicking on a specific website. However, subscribing to the newsletter on the travel company's website does not constitute consent to data processing (Pollirer et al., 2017, p. 32). The request for consent must be written in clear and understandable language and must be distinguished from other facts, such as references to other data protection information (Kastelitz, 2017, p. 110). Consent must often be given for each processing separately, if the information being processed differs from one another. For example, when checking in to a hotel, the consent to send advertisements electronically and the consent to process the passenger's health data must not be contained in the same form.

The subject whose data is being processed can revoke his consent at any time. Unlike the GDPR, which stipulated that a minor who has reached the age of 16 can independently give consent for the processing of personal data, our PDPA lowered that limit to 15 years of age. This means that the consent to send the newsletter of the children's resort to a child who has e.g. 13 years old can only be given by a parent or legal representative.

The most common legal basis for the processing of personal data in the tourism sector is that the processing is necessary for the purpose of executing a contract or undertaking actions leading to the conclusion of a contract. In particular, data about the address of a guest who ordered an information bulletin from a travel company can be entered and saved in the user's file for the processing of the order process.

The legal basis for processing personal data is also the legal obligation of the data handler. The Law on Hospitality of the RS in Art. 7, paragraph 1, point 17 prescribes that the caterer is obliged to enter data about the user of the accommodation service daily and regularly in the prescribed manner. In addition, the same Law in Art. 15 stipulates that the caterer who provides the accommodation service is obliged to enter data about the user of the accommodation service through the central information system, in the prescribed manner. For domestic citizens, these data usually include "name and surname, day, month and year of birth and residential address" (The Law on Hospitality, Art. 15, Par. 2). For foreign nationals, these data include "name and surname, day, month and year of birth, citizenship, type, number and date of issuance of the foreign travel document" (The Law on Hospitality, Art. 15, Par. 3). The above data is entered by the caterer through the central information system (E-tourist) based on the data from the identity card, travel document or other public document with a photo. Through this system, registration and de-registration of tourists is carried out, tourist taxes are paid and facilities are categorized. This system gathers all data on caterers and catering establishments in the Republic of Serbia. All the above data are collected based on legal obligation. However, special consent from the guests is necessary for the use of said data for electronic connection with the system of the local or regional tourist association. In practice, this consent is given in an additional checkbox with appropriate information about data processing for this new, different purpose.

The Ministry of Trade, Tourism, and Telecommunications, as well as the local government unit, collect personal data on natural persons who provide catering services in the manner prescribed by the Catering Act (Art. 64-69) and PDPA.

The processing of personal data is lawful when it is necessary to protect the vital interests of the data subject. In tourism, this basis has little application. A possible example in tourism practice is information about the guest's age, physical ability or eating habits in the event of a medical emergency.

The processing of personal data is also legal if the processing is carried out for the purpose of performing tasks in the public interest or for the purpose of exercising the powers prescribed by law. This basis for the processing of personal data would exist in the event that the local government transfers the obligation of guest registration to the local tourist association. Guest data in this case would be processed by the local tourist association for the purpose of performing tasks in the public interest. A contract between the local self-government and the corresponding tourist association is necessary for the execution of works in the public interest in the above given example.

Personal data must be processed fairly. The principle of fairness aims to direct all those who apply legal norms to take care of every processing, which means that facts and norms are interpreted and applied according to the circumstances of each specific case (Andonović & Prlja, 2020, p. 56). Responsible persons should process other people's personal data with full care and respect. An example from tourism practice is a questionnaire that a tourist fills in at a tourist association and that is forwarded to accommodation facilities in a certain tourist region without their consent in order to send them suitable offers. Instead, it is in the interest of the guest that the tourist association sends him collective offers of accommodation facilities, without the need to send his/her data to various tourist companies in the region.

The principle of transparency allows citizens to be aware of all activities related to their personal data. In essence, transparency means that the processing of personal data is carried out in a way that is understandable to the data subject (Kastelitz, 2016, p. 100). For example, a person who fills out a questionnaire on a tourist site directly from the questionnaire should be clear to whom the questionnaire is intended, to whom it can be transmitted, for what purposes the questionnaire data can be used, i.e. for what other similar purposes it can be further used.

Personal data CAN only be collected on the basis of the reasons provided for in advance by law. In other words, personal data cannot be collected before there is a need for their processing. Limitation in relation to the purpose of processing is one of the central principles of European data protection law. Our PDPA stipulates this principle in Art. 5, Paragraph 1, Point 2. The reasons for processing personal data must be stipulated in advance by law. In certain exceptional situations, personal data may be used for purposes other than those for which they were originally collected. It is a condition that other purposes are compatible with the original purpose of data collection. If this compatibility cannot be established, data processing for other purposes is permitted only with the express consent of the processing subject. For example, specific consent or other legal basis is required to send informational brochures or postal Christmas cards to hotel guests.

When there is a need to process personal data from citizens, only those data that are essential for achieving the purpose of the processing can be requested. For example, on a tourist website, in the questionnaire about available rooms or apartments, the user should not be asked in the mandatory field, e.g. about his occupation.

The principle of accuracy means that data stored in databases must be updated and harmonized with changes in the factual situation (Voigt & Bussche, 2017, p. 91). However, in certain situations it is necessary to save information that has been determined to be incorrect. For example, in specialized hotels that provide medical services, a person's medical record may contain a diagnosis that turns out to be incorrect. Regardless of the fact

that this information is not correct, it will be kept because it is necessary for the further treatment of that person. Of course, in the appropriate place, it is necessary to make a note about the inaccuracy of certain data.

The storage of personal data is limited to the time that is really necessary to achieve the purpose of processing. Data that are no longer necessary must be deleted. Deleting unnecessary data reduces misuse and inaccuracies of data stored. The PDPA sets out the reasons for which personal data may be stored for longer than the purpose for which the data was collected. These are the following reasons: archiving in the public interest, processing in the interest of historical or scientific research. The period of storage of personal data is easy to determine in those cases where the legal basis for the storage of personal data and the erasure period derives from the law (Hötzendorfer et al., 2018, p. 58). In the tourism sector, there is no legitimate interest in storing an email address after sending a brochure ordered by a client via e-mail.

When processing personal data, processors can find out important information about the life of the individual whose data is being processed. Loss, destruction or misuse of personal data by third parties could cause negative consequences for the rights and interests of the person whose data is being processed, as well as those close to him. For example, information about the tourist destination where the clients of a travel company rest and the vacation period is leaked to the public, which can cause harmful consequences for the rights and interests of the clients of that company. Data processing must be secure and secured by special measures that protect against unauthorized access and misuse (Voigt & Bussche, 2017, p. 92).

Personal data must not be accessible to unauthorized persons. An example of the disclosure of personal information in tourism is a list of travelers that is available to a tour guide (Kędzior & Sadowska, 2019, p. 77). In certain situations, it is necessary for the guide to call the passengers. However, it can be disputed here whether the guide is allowed to read the passenger list out loud. Practice on this matter has not yet been established. Bearing in mind that for security reasons the guide reads the list of passengers he received from the tour operator, we believe that in this case the guide does not violate the rules on the protection of personal data.

3.2. Special categories of personal data

There are categories of personal data that may not be processed as a rule. It is about personal data that enjoys a higher degree of protection compared to the protection that is usually provided to personal data. This type of personal data refers to characteristics of a strictly personal nature, the violation or misuse of which may have negative consequences for the natural person to whom they relate. This group includes data related to: racial or ethnic origin, political opinion, religious or philosophical belief, membership in a trade union, genetic and biometric data, data on health or data on the sexual life or sexual orientation of a natural person (PDPA, Art. 17, Par. 1).

Special categories of personal data are regularly processed in the tourism industry. Primarily, it refers to health data. Health data contains information about the "physical or mental health of a natural person, including data on the provision of health services, which reveal information about his health condition" (PDPA, Art. 4, Par. 1, Point 16). The Court of Justice of the EU interprets the concept of health data very broadly, which, according to this court, refers to all information that affects all aspects of human health - both physical and psychological (Hödl, 2018, p. 26). Data on food allergies and intolerances of guests, which are generally regularly recorded in the hotel and catering industry, also belong to health data.

There are several situations in which the processing of special types of personal data is permitted. The first situation is the consent of the person whose data is in question. Another case is that the vital interests of the individual require the processing of his personal data. In tourism practice, the processing of health data is carried out only if the person to whom the data refer has given consent to the processing. Data on food allergies and intolerances are most often of vital importance for the health of the person to whom the data refer. Therefore, these data can exceptionally be processed without the express consent of the person to whom these data refer (PDPA, Art. 18, Par. 1, Point 2).

In addition to health data, a special type of data that is processed in the tourism industry is data on sexual orientation, that is, the life of a certain person. An example of this is the registration for an event that is expressly organized for persons of homosexual orientation, based on which a conclusion can be drawn about the sexual orientation of those present at that event.

3.3. Rights of natural persons concerning personal data

The PDPA regulates institutes and issues of importance for the protection of personal data in Serbia. As special rights related to the protection of personal data, the Law singles out: the right to information, the right to correction, the right to be forgotten, the right to limit processing, the right to transfer data, and the right to object (PDPA, Art. 21-40).

The right to information gives individuals the opportunity to obtain information on all matters related to the processing of their personal data (Davinić, 2018, p. 52). PDPA envisages the right to be notified by art. 23 determines the range of information provided to the person from whom personal data is collected. The right to information provides data subjects with transparency regarding their personal data being processed. In this context, a natural person has the right to information on whether the processing of his personal data was carried out in a clear and comprehensible form, in writing, orally or electronically. The information must be provided electronically if the request for information is submitted electronically (e.g. by email). Exceptionally, the answer can be given in a different form only if the person concerned agrees to it (Feiler & Horn, 2018, p. 85). Especially in the case of giving information orally, the identity of the person requesting the information should be checked before giving the information. The data must not be given to a person who is not authorized to receive the information. Otherwise, the principle of data confidentiality would be violated. On the other hand, it should not be unnecessarily difficult for a certain person to exercise his right to information (Haidinger, 2016, p. 126). However, if, for example, a person requests information via e-mail about the saved data about the use of his electronic guest card during the last holiday and mentions only his name and the holiday period, the identity of this person should be verified with additional authentication measures, provided that the guest is not clearly identified in the system guest's electronic cards via the e-mail address.

The right to correction and addition of personal data is regulated in Art. 29 PDPA. The right to correction is based on the fact that every natural person has the right to request the correction of incorrect or inaccurate personal data. Correction is required from the person who stores and uses the data. In addition to the correction, natural persons can also request the addition of personal data. Personal data is used daily in the tourism sector for identification, the conclusion of contracts, and realization of various tourist services. A natural person has the right to request the responsible person to immediately correct incorrect data or to request the completion of incomplete data. For example, if a name is misspelled in a holiday reservation, the person responsible is obliged to correct this information. A correct and up-to-date database is also in the interest of responsible persons.

A natural person has the right to request the responsible person to delete his personal data in the cases prescribed by the PDPA in Art. 30, Paragraph 2, Points 1-6. For example, the purpose for which the data was collected has been achieved or the data processing has been carried out in violation of the law. In addition, it may happen that a natural person withdraws consent to processing. In all these cases, the person whose data is in question can request the deletion of the data. According to the law, tourist companies are obliged to store certain personal data, e.g. documents used in accounting. This means that the guest cannot request the deletion of personal data stored in the hotel's accounting (e.g. booking confirmation and hotel invoice). The request for deletion of this data can be rejected with reference to Art. 12, Paragraph 1, Point 5 PDPA. The request for deletion can also be rejected if the processing of personal data is a necessary condition for the realization of the legitimate interests of the responsible person. For example, if incidents occurred during the stay at the hotel that could justify a claim for damages by the hotel against the guest, the guest's request for deletion of personal data may be rejected with reference to Art. 12, Paragraph 1, Point 6 PDPA.

A natural person has the right to request that the processing of his/her personal data be limited by the responsible person if one of the cases stipulated by the PDPA in Art. 31, Paragraph 1, Points 1-4. One of those reasons is that the personal data are no longer necessary for the responsible person to achieve the purpose of the processing, but the person to whom the data refers has requested them in order to submit, exercise or defend a legal claim. For example, a hotel has filed a claim for damages against a hotel guest. The guest has the right to object to the deletion of any video material from the hotel, if he believes that the video material could serve as evidence in the court proceedings the hotel is conducting against him.

The right to data portability gives citizens the opportunity to demand that the entity that disposes of their data transfer it to another entity. In the tourism sector, this right does not have much importance, except in some exceptional cases. For example, the guest has the right to request that the hotel transfers his personal data in case he decides to change hotels.

PDPA in Art. 37 regulates the right to a remedy. Every person has the right to object to the processing of personal data relating to him. The right to object is of great importance in the tourism industry, especially in direct marketing, i.e. advertising.

4. Rights related to automatic processing of personal data

The development of modern technologies has led to the "independent" operation of computers. Computer programs that automatically predict results have proven to be useful tools in making various business decisions, remediating economic losses, and in the decision-making process in everyday matters. Automatic decision-making is used in finance, education, medicine, tourism, and many other areas.

Artificial intelligence technology (hereinafter: AI) has, among other things, the ability to predict, i.e. give recommendations. This ability is based on the ability to use information, that is, data to classify and evaluate different individuals. Thanks to AI, business entities can adapt their products or services to each individual. Unlike traditional software, AI technology can even predict the behavior of individuals. Thanks to this, business entities can provide and improve the range of their products and services, adapting them to the habits and needs of individual clients.

AI-based personalization has the power to improve the quality of travel services as well. Travel companies can use AI to offer their customers personalized recommendations for their services. Namely, tourists are increasingly searching for tourist destinations online, booking travel and accommodation. As a result of this growing trend, tourism companies

have new ways i.e. chances to connect with customers. Thanks to AI-based personalization travel companies can adapt their services to suit the requirements, habits, and preferences of each customer.

AI can generally be used to customize the user experience as it can collect, analyze and combine large amounts of data from different sources. Thanks to this, AI can be more effective than traditional personalization techniques. However, AI-based personalization has its drawbacks. Namely, successful personalization requires high-quality data. If the data is missing or incorrect, AI can make recommendations and offers that do not match the individual profile of the client, i.e. it can give results that can lead to unjustified divisions between people, discrimination, labeling of people, and similarly. On the other hand, entities including travel companies that want to increase personalization must take into account the privacy of clients, i.e. comply with regulations on the protection of personal data. Excessive personalization can negatively affect the user experience. Despite the challenges, AI-based personalization is being used in the tourism sector to understand user habits and needs in order to generate personalized travel service recommendations with greater precision. In the tourism sector, especially in smart tourist destinations, chatbots, and virtual assistants are popular that answer the queries of individuals, help them find their way on a certain website, and suggest personalized services (accommodation, transportation, destinations) that clients might be interested in (Masseno & Santos, 2019, p. 8). Thanks to data such as travel history, purchase history, and loyalty program status, the AI-based system will provide personalized offers according to the budget and habits of individuals.

AI has the potential to improve not only the quality of business but also the quality of people's lives. However, AI-based personalization opens up a dilemma – how and where to draw the line between personalization and privacy? In order to protect citizens from the unwanted consequences of automatic decisions by computer programs, data protection systems recognize citizens' special rights in relation to such decision-making. This is also the case with the legal system of Serbia, in which the right of a person to decide whether a decision made solely based on automatic processing of personal data will be applied to him is guaranteed, i.e. from the processing done by the computer program (Art. 38, Para. 1 PDPA). The decision must have a certain legal significance, so only those decisions that produce legal consequences or that significantly affect the rights and interests of a certain natural person are taken into account.

In addition to automatic data processing, citizens have the right to decide whether decisions based on "profiling" will be applied to them. Profiling is defined as "any form of automated processing that is used to assess a specific personality trait, in particular for the purpose of analyzing or predicting a natural person's work performance, economic position, state of health, personal preferences, interests, reliability, behavior, location or movements" (Art. 4, Paragraph 1, Point 5 of the PDPA).

Health tourism can be cited as an example of decision-making based on profiling and automatic data processing. Computer programs in healthcare can classify a certain person in the category of persons most susceptible to thyroid disease and who is therefore recommended to stay at Zlatibor in Čigota - the Specialized Hospital for thyroid diseases. This profiling does not mean that the person already suffers or will suffer from thyroid disease. Aware of the need for special nutrition for thyroid patients, Čigota Specialized Hospital provides personalized meals in accordance with the health condition of the patients (Masseno & Santos, 2018, p. 127).

The person whose data is used in automatic data processing must have the opportunity to express his position regarding the specific decision, as well as to invest in legal remedies if he believes that the decision is not correct or legal. However, the operator must also take

adequate measures to protect the rights and interests of the person whose data is used in automatic data processing, such as the inclusion of the human factor in the control of the automated processing process.

Thanks to this right, citizens have the opportunity to decide independently whether to accept personalized results that are obtained based on automatic data processing. In this way, the basic principles of personal data protection, such as transparency, legality of processing, and protection of the legitimate interests of the person whose data is processed, are realized. However, in certain cases, citizens cannot avoid the application of the results of automatic data processing (Art. 38, Para. 2 PDPA). The first case refers to decisions made based on a special regulation that allows automatic data processing. The second case refers to decisions that are necessary for the conclusion or execution of a contract between the person to whom the data refer and the controller. The third case refers to giving express consent to the automated processing of personal data.

In addition to the contract, the basis for automatic data processing can also be a special regulation. In this way, it is possible to enable the automatic processing of personal data as a rule in certain cases, when administrative bodies perform important social tasks (such as public health or national security). However, the regulation that allows automatic data processing must be specifically explained, based on the legitimate expectations of citizens and in accordance with the data protection system.

5. Results and discussion

The topic of personal data protection is a challenge for many travel companies. Travel agencies, caterers, as well as travel and accommodation booking platforms process a large amount of data every day. In accordance with the regulations on the protection of personal data in tourism business, it is important that personal data is inaccessible to others. With the constant traffic of tourists reigning in tourist facilities, data should be well secured. Therefore, tourist entities should first of all protect their computers from access by others. Secure passwords and a good firewall form the cornerstone of IT security in tourism. In addition, very simple things, such as a privacy screen on the computer that blocks the view of other guests' reservations, should be a standard in tourism. However, in addition to the protection of digital data, it is important to implement protection when collecting analog data. Despite the fact that more and more work is done digitally and that the protection of personal data is often equated with the protection of digital data, handwritten data must also be secured. In this sense, cabinets or offices must be locked and documents must not be visible at the reception desk. In general, reception and reservations are the key factor to data protection. In many cases, the so-called tourist tax must be paid. It is not uncommon for there to be forms that must be filled out manually when signing up. And this data must be protected, i.e. provide in an adequate manner.

The implementation of regulations on the protection of personal data in tourism is no different from other business areas. A special challenge in meeting the requirements for the protection of personal data exists on the part of international companies. Namely, hotel guests are often people with foreign citizenship. In this sense, it is necessary that the obligation to notify and statements on data protection be available at least in English. This is the only way to ensure that all interested parties can exercise their data protection rights and understand the purpose of their data collection.

The protection of personal data also applies to online platforms. Therefore, if the reservation of travel, accommodation, etc. is performed through an external booking platform, it must be checked in any case to what extent a contract for the processing of personal data is necessary

in the sense of Art. 45 PDPA. In addition, it is important that data is sent only through secure and encrypted access. However, the processing of personal data is not only a process carried out during a reservation or enquiry. Each collection, for example, of a potential customer's IP address, each cookie setting and related data processing constitutes a collection of personal data that is subject to personal data protection. Therefore, travel companies are obliged to use their website in accordance with the regulations on the protection of personal data.

Personal data is not processed only when booking and checking in to a hotel or apartment. Video surveillance is a classic example of the further collection of personal data. Photographs may also constitute personal information if the person concerned is clearly identifiable in the image. Recording of any kind is part of the processing of personal data. Numerous tourist facilities, primarily hotels, use surveillance cameras citing a legitimate interest, such as the safety of employees, protection against burglary, and protection of property or vandalism. A clearly visible sign must be placed in front of the area monitored by the camera, indicating that the area is being monitored.

6. Conclusion

The PDPA contains the rules and basic institutes within the personal data protection system in Serbia. This law has largely aligned personal data protection standards with GDPR as a regulation that has direct application in all EU member states. However, data protection rules and institutes can also be found in other regulations that govern specific areas of social life. In the tourism sector, these are the provisions of the Law on Tourism (Articles 113-118) and the Law on Hospitality (Articles 64-69).

Travel companies collect various personal data in their work. Despite the fact that the domestic and European regulations on the protection of personal data contain certain legal gaps, most companies, including tourist companies, have learned to act appropriately in relation to the application of the regulations on the protection of personal data. However, adaptation of all companies, including tourist companies, to the rules and requirements on the protection of personal data must be done continuously. Every day, various entities collect large amounts of personal data, store them in large databases and process them. With the growth of collected data, the danger of its misuse has also increased. In addition to an effective legal system for the protection of personal data, it is extremely important to establish high-quality personal data security measures. These measures must also be implemented in the tourism sector. Employees in the tourism sector must have good self-control skills. In addition, continuous practical training in the field of personal data protection is necessary. In this sense, this paper represents a contribution to raising awareness and understanding of the meaning and purpose of personal data protection in the tourism sector.

In general, many open questions related to the protection of personal data will be clarified by case law. In the field of electronic communication, it can be expected that the planned new EU Directive on e-Privacy will create significantly more legal certainty in the field of personal data protection on the Internet. Namely, this Directive is primarily intended for companies operating in the digital economy and specifies additional requirements that these companies should fulfill in connection with the processing of personal data.

Conflict of interest

The author declares no conflict of interest.

References

1. Andonović, S., & Prlja, D. (2020). *Osnovi prava zaštite podataka o ličnosti [Basics of the right to protection of personal data]*. Institut za uporedno pravo, Beograd, Srbija.
2. Buhalis, D. (2020). Technology in tourism-from information communication technologies to eTourism and smart tourism towards ambient intelligence tourism: A perspective article. *Tourism Review*, *75*(1), 267–272. https://doi.org/10.1108/TR-06-2019-0258
3. Chatzopoulou, C. I. (2021). GDPR and tourism: Legal framework, compliance and implications for the tourism industry. *Economy & Business Journal*, *15*(1), 125–133.
4. Davinić, M. (2018). *Nezavisna kontrola tela u Republici Srbiji [Independent body control in the Republic of Serbia]*. Dosije studio, Beograd.
5. Feiler, L., & Forgó, N. (2016). *EU-DSGVO: EU-Datenschutz-Grundverordnung*, Austria.
6. Feiler, L., & Horn, B. (2018). *Umsetzung der DSGVO in der Praxis*, Austria.
7. Fercher, N., & Riedl, E. (2016). Entstehungsgeschichte und problemstellungen aus österreichischer Sicht. In R. Knyrim (Ed.), *Datenschutz-Grundverordnung DSGVO - Das neue Datenschutzrecht in Österreich und der EU* (pp. 7–30). Austria.
8. García, L. M., Aciar, S., Mendoza, R., & Puello, J. J. (2018). Smart tourism platform based on micro service architecture and recommender services. In M. Younas, I. Awan, G. Ghinea, & M. Catalan Cid (Eds.), *Mobile Web and Intelligent Information Systems* (pp. 167–180). Springer International Publishing. https://doi.org/10.1007/978-3-319-97163-6
9. *General Data Protection Regulation 2016/679 (EU GDPR)*. Retrieved June 15, 2022 from https://gdpr-info.eu/
10. Gretzel, U., Reino, S., Kopera, S., & Koo, C. (2015). Smart tourism challenges. *Journal of Tourism*, *16*(1), 41–47.
11. Haidinger, V. (2016). Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit. In R. Knyrim (Ed.), *Datenschutz-Grundverordnung* (pp. 125–136). Austria.
12. Hladjk, J. (2016). Sachlicher und räumlicher Anwendungsbereich der DSGVO. In R. Knyrim (Ed.), *Datenschutz-Grundverordnung DSGVO – Das neue Datenschutzrecht in Österreich und der EU* (pp. 39–41). Austria.
13. Hödl, E. (2018). Art 4 DSGVO. In R. Knyrim (Ed.), *DatKomm*. Austria.
14. Hötzendorfer, W., Tschohl, C., & Kastelitz M. (2018). Art 5 DSGVO. In R. Knyrim, (Ed.), *DatKomm*, Austria.
15. *Judgment of the First Senate of 15 December 1983 - 1 BvR 209/83*. Retrieved July 30, 2022 from https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html
16. Kastelitz, M. (2016). Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten. In R. Knyrim (Ed.), *Datenschutz-Grundverordnung DSGVO - Das neue Datenschutzrecht in Österreich und der EU* (pp. 99–114), Austria.
17. Kędzior, M., & Sadowska, M. (2019). General data protection regulations: Opportunities and risks of the implementation of GDPR in tourism. *ACC Journal*, *25*(3), 71–81, https://doi.org/10.15240/tul/004/2019-3-006
18. *Law on Hospitality (Official Gazette of RS, No. 17/2019)*. Retrieved July 15, 2022 from https://www.paragraf.rs/propisi/zakon-o-ugostiteljstvu.html
19. *Law on Personal Data Protection – PDPA (Official Gazette of RS, No. 87/2018)*. Retrieved July 10, 2022 from https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

20. Masseno, M**.** D., & Santos, C. (2018). Smart tourism destination privacy risks on data protection: A first approach from a European perspective. *Revista Eletrônica Sapere Aude*, *1*(1), 125–149.
21. Masseno, M. D., & Santos, C. (2019). Personalization and profiling of tourists in smart tourism destinations – A data protection perspective. *International Journal of Information Systems and Tourism*, *2*, 7–23.
22. Pollirer, H. J., Weiss, E. M., Knyrim, R., & Haidinger, V. (2017). *DSGVO, Datenschutz-Grundverordnung.* Austria.
23. Voigt, P., & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer eBook, Switzerland. https://doi.org/10.1007/978-3-319-57959-7

Received: 22 March 2023; Revised: 16 May 2023; Accepted: 2 June 2023