GENERAL DATA PROTECTION REGULATION: OPPORTUNITIES AND RISKS OF THE IMPLEMENTATION OF GDPR IN TOURISM

Mariusz Kędzior[1]; **Mirela Sadowska**[2]
Wrocław University of Economics,
Faculty of Economics, Management and Tourism in Jelenia Góra,
ul. Komandorska 118-120, 53-345 Wrocław,
Filia w Jeleniej Górze, ul. Nowowiejska 3 58-500, Jelenia Góra
e-mail: [1]mariusz.kedzior73@gmail.com; [2]mirela.sadowska@ue.wroc.pl

Abstract

The article is an attempt to answer the most frequently asked questions regarding the processing of personal data in the tourism industry. It is an attempt to explain the basic definitions regarding the protection of personal data. It specifies duties that should be fulfilled by organisers, tour operators and hotel and boarding house owners in order to ensure that the processing of data of natural persons is in line with the GDPR. It also specifies risks connected with personal data processing and opportunities to ensure the security of data processed by tourism service providers.

Keywords

Personal data protection; Tourism; Tourist traffic; Hospitality.

Introduction

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (abbreviated GDPR) [1] came into force on 25 May 2018. This has raised numerous questions regarding what kind of data can be collected and how they should be stored and shared. All organisations that process personal data of natural persons are obligated to obey the rules outlined in the Regulation. This includes business entities such as travel agencies, tour operators, guides and hotels. The data collected by such businesses from customers are diverse, ranging from their full name, address, national identification number and age to information about their dietary requirements, medical conditions or even religious beliefs. Such data are collected in order to ensure maximum comfort to the travellers. The provision of package travel sometimes requires the transmission of data to other entities, for example to a hotel for the purpose of assigning rooms to guests or to an insurance provider in order to make an insurance contract.

In order to properly implement the GDPR, it is necessary to choose an appropriate mode of action, prepare the correct documents and procedures, analyse the risks connected with the processing of personal data and continuously improve the system. The implementation of the system is a difficult task considering that it requires a thorough diagnosis of the functioning and environment of the given organisation that processes personal data. Current data protection regulations leave room for interpretation, which, in the event of a misunderstanding, may jeopardise the organisation and lead to financial penalties being imposed. Only a comprehensive approach based on risk management and an analysis of the processes in place provides the means for an effective implementation and application of the

GDPR that ensures the protection and enforcement of the rights of the individual and guarantees legal security of the organisation as a whole.

Because of the way it is formulated, the new regulation does not impose ready-made solutions or prescribe the implementation of unadjusted criteria from the top down. Each action is to stem from the individual circumstances and requirements of the given organisation that processes personal data. The implemented safeguards should be adequate, which means they should successfully ensure data security, especially in organisations involved in large-scale processing of personal data of natural persons, such as tourism and hospitality enterprises.

The article aims to present the historical background of personal data protection, explain terminology related to the categories of the personal data being processed, as well as outline the new duties faced by the tourism industry as a result of the introduced changes. The article is based on an overview of literature and professional press, as well as an analysis of existing Polish and international research and legal acts in force in Poland and the European Union.

1 The GDPR: a Terminological Perspective

One of the main reasons the introduction of the Regulation was deemed necessary by the European legislator is the socio-economic integration of the EU member states, which results from the functioning of the internal market and has led to a considerable increase in cross-border data flows. This increase applies to all types of entities, both public and private, in particular to natural persons and commercial law companies. One must certainly also note the direction of the evolution of European law, which has in recent years increasingly required EU member states to cooperate and exchange personal data in order to fulfil their own duties or act on behalf of another member state.

Another factor that certainly contributed to the introduction of the Regulation is the new challenges in personal data protection stemming from ubiquitous globalisation and rapid technological progress. These phenomena have considerably influenced the personal data processing capabilities of public and private law entities, which are now able to use various categories of data at an unprecedented scale. Such changes require a stable, more consistent framework for data protection in the EU, as well as strict enforcement of such protection. Building trust is vital to the development of the digital economy on the internal market, and an integral part of such trust is natural persons' ability to be in control of their own personal data, as well as legal and practical certainty for all categories of private and public entities.

From 25 May 2018 onwards, all enterprises, authorities, schools, non-government organisations, as well as tourism-related service providers will be obligated to comply with the requirements of the GDPR. Exempt from the new regulation is only the processing of personal data in the course of purely personal or household activities. [4, p. 22] One must be aware that the implementation of the Regulation is important not just for entrepreneurs, but for consumers as well. In practice, besides imposing a variety of requirements on companies that process personal data, the GDPR grants customers numerous rights that allow them to protect their privacy. Data subjects gain new rights, while controllers – i.e. personal data processors (in this case hotels) – are assigned new duties. The GDPR also introduces financial penalties for breaching its provisions. In the beginning, one must note that the hotel industry is a sector where the scale of personal data processing is very large. An average hotel processes a wide variety of personal data belonging not only to its guests, but also to its employees. Besides obvious information such as the individuals' full names, such information may include location data, the guests' phone call history or likenesses (photographs) captured by surveillance cameras installed in the hotel. If a hotel records phone calls, the list of data being processed also includes voice, which constitutes biometric data.

The rapid development of information technology that has taken place over the last decade and continues to this day made it necessary to take an entirely new approach to personal data protection. The widespread access to personal data provided by information technologies resulted in such data becoming a commodity and being used for unlawful purposes. For that reason, the socio-economic phenomenon that is personal data processing required the introduction of regulations that would improve security in this regard. There was also a need for standardisation of the previously used regulations. Each EU member state had been processing personal data in a different way. This would result in situations where numerous issues would arise from inconsistencies in regulations. The new personal data protection policy is the same for each EU member state and also has to be applied by countries that co-operate with the European Union, such as the United States of America.

As is the case with every socio-economic phenomenon, personal data processing could function with no pertinent regulations in place. This, however, could lead to various kinds of abuse and unauthorised processing of personal data. One example of a socio-economic phenomenon that, like personal data processing, has required regulation, is road traffic. When motor vehicles were introduced, road traffic had not yet been regulated. The rapid development of the automotive industry, the increasing number of vehicles in use and pedestrians walking on public roads in combination with a lack of standardised traffic laws resulted in numerous road accidents. Traffic laws, established in response to the development of transportation, have not solved all traffic-related problems; however, they have limited the number of accidents and made driving and pedestrian traffic much safer.

The GDPR is similar. The development we are currently witnessing is nothing short of an information revolution. The widespread access to personal data of natural persons has often provided opportunity for abuse, such as the unlawful assumption of financial liabilities in the name of another person without their knowledge. Major companies, such as banks, service providers and other data processors, have also struggled with large-scale data breaches. In response to such threats, the European Parliament has resolved to introduce new regulations in order to protect personal data.

2 Categories of Personal Data

According to Article 4(1) of the GDPR [1], ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Previously, protected personal data were limited to two categories. One of them consisted of regular personal data, including a person’s full name, physical address, national identification number, e-mail address and computer IP address. A separate category was constituted by sensitive personal data. These included information about a person’s ethnic origin, health (medical data), religion, as well as political or trade union affiliation. Now, the list of protected data has been extended to include biometric data, such as fingerprints, voice recordings or iris scans, as well as genetic data, which refers to information stored in a person’s genetic code. The distinction has major consequences in terms of the technical and organisational measures employed in order to process individual categories of personal data, since the classification of personal data as sensitive significantly raises the requirements regarding the protection of such data.

A new solution introduced by the GDPR is the distinction of special categories of personal data:

- **genetic data** – personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, [1, Article 4(13)]
- **biometric data** – personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, [1, Article 4(14)]
- **data concerning health** – personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. [1, Article 4(15)]

The division of personal data into two categories has also an effect on the available legal bases for the processing of such data. Data classified as sensitive (a special category of personal data) cannot be processed based on a contract or a legitimate interest of a controller. [1, Article 6 – Lawfulness of processing] The basic ground for the processing of personal data is the consent of the data subject. It is worth noting that the GDPR puts great emphasis on the conditions of valid consent. Other grounds include the necessity to perform a contract or the fulfilment of legally justifiable purposes by data controllers. In principle, although the GDPR uses slightly different wording, it repeats the current legal bases for personal data processing and adds an additional one: "vital interests of the data subject", currently used exclusively in the case of the processing of sensitive data. The GDPR is the first to explicitly formulate rules governing children's consent to data processing, stating that in the case of "information society services" (in simple terms, services provided by electronic means) such consent can be given by a child 16 years of age or older; otherwise, such consent must be given or authorised by the holder of parental responsibility over the child. At the same time, the GDPR allows EU member states to provide by law for a lower age limit, provided that such lower age is not below 13 years. Poland is one of the countries to have done so. [2]

3 Disclosure Requirement in the Tourism Industry

One of the main obligations imposed on data controllers by the GDPR is the requirement to provide information to the data subject in certain situations. [3, p. 245] In comparison with the "old" personal data protection act, the European legislator has significantly expanded the list of information that has to be provided to such a person.

Following the entry of the GDPR into force, data subjects have the right to obtain a wide array of information regarding the processing of their personal data by the controller. Recital 60 of the preamble of the GDPR states that the data subject must be informed of the existence of the processing operation and its purposes. Furthermore, the controller must provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context of the processing operation.

In general, as per the GDPR, the disclosure requirement must be fulfilled in two situations. The first of these situations is when the data are collected directly from the data subject; the second one is when they are obtained from intermediate sources, i.e. not from the data subject. In the case of the collection of data from the data subject, the GDPR does not prescribe a format or procedure to be followed when disclosing such information; however, it clearly indicates that the implementation of "suitable measures" regarding disclosure is the responsibility of the data controller. It must be therefore concluded that the required information must be provided to the data subject either at the time of the collection of data (at the latest) or directly before collection. The disclosure requirement does not discriminate

between methods of data collection, which may include e-mail, fax and other means of communication. In situations where the data controller collects personal data using forms, the disclosure requirement may be fulfilled by including relevant information in the form itself.

If data are collected from a source other than the data subject, the data subject must be informed about this fact within a reasonable period, however no later than within a month. [1, Article 14(3)(a) and Recital 61 of the Preamble of the GDPR] If personal data are to be used for the purpose of communicating with the data subject, the disclosure requirement must be fulfilled at the time of the first such communication at the latest. In cases where the controller plans to disclose personal data to another recipient, the controller is obligated to inform the data subject about this fact at the time of the first disclosure of such data to the new recipient. [1, Article 14(3)(c)] The above provision applies to situations where personal data are obtained from an entity other than the data subject and is also referred to as secondary data collection.

The disclosure requirement must be fulfilled in situations where personal data are collected directly or indirectly from the data subject. [1, Articles 13 and 14] The concept of data collection is not defined in the provisions of the Regulation. One can define it as a set of operations that constitute the processing of personal data, such as each procurement of such data with the intention of further processing, regardless of whether such processing will take place within a filing system. The procurement of personal data is of key significance in this situation: regardless of whether such data have been voluntarily submitted by the data subject or obtained in another manner, the disclosure requirement must always be fulfilled. The GDPR distinguishes two situations in which personal data collection may take place, based on the aforementioned article [1, Article 14] (primary and secondary data collection). The aforementioned provisions shape the disclosure requirements imposed on the data controller depending on the data source and the controllers' relationship with the data subject.

The data controller [3, pp. 134–147] is also required to provide the data subject with relevant information when acquiring new (from the controller's perspective) personal data. This means that the controller should fulfil the disclosure requirement not only when collecting data from the data subject, but also when intending to collect new data from the same subject that was not collected at the time of the first contact. This is why the collection of new data should be understood as an expansion of the set of data already in the possession of the controller to include new categories of information about the data subject. In this situation, the controller is obligated to once again provide the subject of the newly collected data with the required information. There is, however, an exception to the above rule: the disclosure requirement does not need to be fulfilled if the collected data are merely updated or removed as a result of actions performed by the controller or the data subject. In the above case, the controller is not obliged to fulfil the disclosure requirement, as no new categories of data are collected; however, nothing prevents the controller from providing the data subject with relevant information.

Another situation where the fulfilment of the disclosure requirement is obligatory is a change in the purpose of data processing. If the purpose of personal data processing changes to one that is different from the purpose for which the data were originally collected, the controller must inform the data subject about the new purpose. Where the controller intends to further process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information, as mentioned in paragraph 2 of the aforementioned provisions. [1, Articles 13(3) and 14(4)]

4 Selected Issues Related to Personal Data Processing in the Tourism Industry

The tourism industry will fully come under the provisions of the GDPR, which, in accordance with the principles of EU law, have priority over the laws of individual member states and will be applied directly. Of particular significance to the hotel industry may be the obligation to inform the data subjects about the existence of the data processing operation in a fair and transparent manner. Furthermore, in situations where data are obtained from third parties (e.g. travel agencies), the hotel will have no more than a month to fulfil the disclosure requirement. At the same time, the controller will be obligated to prove that the implemented measures insure the integrity, security, minimisation, confidentiality and accuracy of the data, as well as that the processing thereof will be carried out in accordance with the law.

An example of personal data being disclosed is a list of travel package participants made available to a guide. If all the participants know each other, this is not a problem – they can check on their own if everyone has made it to the meeting spot or onto the coach. An issue arises when a roll call needs to be taken. This leads to a question: can the guide read the list aloud in the presence of other participants? Answering the question is quite problematic since case law and judicial practice are not yet well-established. Nevertheless, for security reasons, taking a roll call is acceptable. The Polish Personal Data Protection Office has confirmed that taking attendance in schools is not in breach of the GDPR. By analogy, taking a roll call of trip participants by reading aloud a list supplied by the tour operator does not constitute a violation the GDPR either.

The obligation to report personal data breaches to the supervisory authority (in Poland, the Personal Data Protection Office) has been a subject of significant controversy. [1, Article 33] Breaches must be reported within 72 hours. One may venture to call such a report a kind of self-denunciation. Having determined that a data breach has occurred in the organisation, the controller, considering the aforementioned large scale of data processing, will be obligated to notify the supervisory authority about the scale of the breach. The expected result of a report may include an ex officio inspection and thus a risk of incurring a fine specified by the GDPR. [3, pp. 316–327]

Depending on the number of employees, data processors may need to appoint a data protection officer selected based on his or her professional qualifications, particularly expert knowledge of the law and data protection practices, as well as aptitude for the relevant tasks. [1, Article 37(5)] The knowledge level of the data protection officer should be determined in the context of the specific requirements of the data controller and processor. [1, Recital 97] As indicated by the Article 29 Working Party, the expert knowledge level, although not specifically determined, must be adequate for the nature, complexity and amount of data processed within the unit. This means that the choice of the data protection officer should be made with due diligence and regard to the nature of the personal data processing carried out within the unit. For public bodies, the appointment of a DPO is mandatory. In the case of commercial entities, the services of a single DPO may be used by several organisations. However, organisations with 250 or more employees are also obligated to appoint a DPO.

The GDPR does not provide for special regulations concerning the tourism industry. It does not introduce any particular data processing requirements that would be less strict than in the case of other industries. [3, pp. 76–81] This means hotel owners will fully come under the provisions of the GDPR, which, in accordance with the principles of EU law, have priority over the laws of individual member states and will be applied directly. The tourism industry is currently facing the challenge of adjusting its procedures to comply with the GDPR. It is not an exaggeration to say that issues related to personal data protection should currently be

treated as a priority by hotel and boarding house owners, package travel agencies and other tourism-related service providers.

Most importantly, operators will need to verify the legal basis for the processing of personal data in the organisation and, if necessary, obtain new consent from customers. Operators must also ensure the fulfilment of the disclosure requirement by providing relevant information to all data subjects. Another important step is the verification of data entrustment agreements with agents, guides, online vendors and all other entities the operator works with. It will also be necessary to evaluate the technical and organisational safety measures taken by such entities when processing personal data controlled by the operator. In addition, the tour operator should verify the legal basis for personal data processing; in particular, check if any new consent needs to be obtained from the data subjects (e.g. for marketing purposes). [3, pp. 200–213]

A key element of the tourism industry is cooperation between service providers. If processing is entrusted to another entity, the data processors should enter into relevant agreements. [6] From this point on, the processor begins to process the data on behalf of the controller. The controller is responsible for ensuring that the processor complies with the GDPR.

An important issue is the existence of a data processing entrustment agreement between the tourism service provider and online booking sites such as Booking or Trivago. If a travel agency has separate agreements (including provisions concerning the entrustment of personal data processing) with tour operators whose products it sells through online channels, it is not required to separately regulate the issue of personal data processing. However, if no such provisions are present in the tour operator agreements, the agency should regulate this matter in agreements with sites such as OnlineGDS [7] or MerlinX [8]. The GDPR introduces new obligations in the relationship between the entrusting and processing parties and enforces the personal data processing principles specified in the new regulations. For that reason, in such a case, it is recommended to sign new agreements.

5 Risk of Personal Data Breach in the Tourism Industry

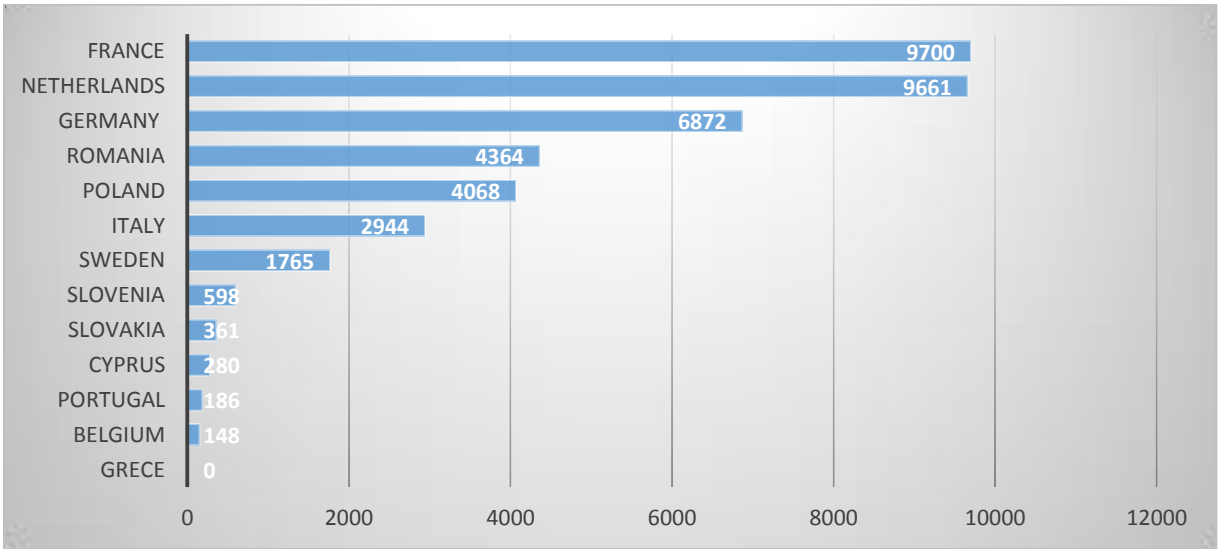
In a situation where personal data are processed repeatedly in order to fulfil a package travel contract, the risk of breaching the regulations should be considered to be high. With that in mind, businesses should establish precise rules to avoid, detect and quickly respond to breaches. Particular protection should apply to genetic, biometric and medical data. It is mandatory to obtain consent before processing such data, regardless of whether the processing arises from a previously made package travel contract. Handling customers' passports, obtaining information about their health or assisting them in medical emergencies may thus cause risks concerning GDPR compliance. In such events, it is required to obtain customers' consent and inform them about their rights. This is also the case in situations where data processing extends beyond the scope of the contracts made, e.g. when it is carried out for marketing purposes.

Considering the increasing popularity of online tourism service marketplaces and digital sales support tools, one must emphasise that automated data processing is subject to the GDPR regardless of whether it takes place within a filing system. Non-systemised data aggregation, such as saving copies of contracts separately on servers or local drives, is thus subject to the provisions of the Regulation even though no distinct filing system exists.

A year after the GDPR entered into force, EU member states are conducting inspections aiming to verify whether the implemented rules are obeyed by the entities subject to them. Poland's first serious penalty for breaching the GDPR has already been imposed. The fine, amounting to PLN 940,000, was imposed by the Head of the Personal Data Protection Office

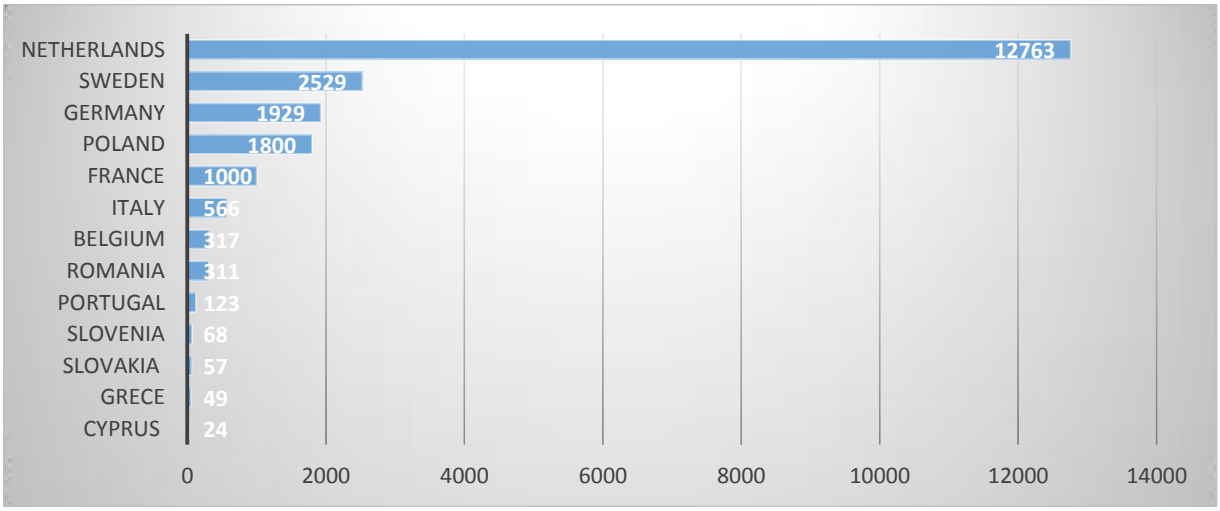
as the first since the GDPR came into force. The breach consisted in failure to provide relevant information to the data subject. Not even the fact that the data originated from publicly available sources, such as the CEIDG (Central Registration and Information on Business), could save the company from the fine. [9] The lack of information prevented numerous persons from exercising their right to have their data deleted or rectified. The company fulfilled its obligation only in the case of persons whose e-mail addresses it possessed. This means the controller knew about the disclosure requirement, but failed to fulfil it in the case of the persons whose e-mail addresses were not on file. This influenced the decision to impose such a high penalty. In defence the company claimed that the costs of notifying the persons via registered mail would have been too high. [5]

The charts in Figures 1 and 2 show the numbers of complaints filed and personal data breaches in EU countries.



Source: [10]

Fig. 1: *Number of complaints filed*



Source: [10]

Fig. 2: *The total number of notifications of data protection breach*

Conclusion

When processing personal data in the tourism industry, it is vital to analyse the associated risks. In situations where such processing may seriously jeopardize rights or freedoms of

natural persons, it is necessary to carry out a data processing impact assessment. Only following such an assessment can the business owner decide whether and to what extent to implement data protection mechanisms, how to use disclosure forms and consent templates, how to draft and sign data processing entrustment agreements, how to maintain records of processing activities and data breaches, how to establish a uniform data processing policy etc.

One thing is certain. The implementation of the GDPR in EU member states, including Poland, and therefore also the adaptation of all businesses (including tourism companies) to the GDPR is a continuous process. The progress that has been taking place in the IT industry has and will have a direct effect on data processors. Companies in the tourism industry, which process personal data on a large scale, should be aware of the surrounding risks for their own security. On the other hand, the implementation of the GDPR is an opportunity for greater control of the data flow and more secure processing. The security of the personal data processed in the tourism industry depends principally on the people in charge of the processing activities. Therefore, it is vital that such people possess good self-control skills and are provided with constant training and support concerning practical knowledge.

An opportunity presented to the industry by the introduction of the GDPR is the increased protection of consumers' personal data. Data protection is to be built into the data processing system by design and enabled by default. [1, Article 25] By implementing the principle of data protection by design, businesses can give users a sense of security: when using a mobile app or website or participating in a contest, users can be sure that the data controller already took measures to protect their data at the design stage. Another benefit for businesses is the opportunity to build consumer trust and their image as reputable companies. The new regulations adopted by the EU are intended to mobilise businesses to take a modern approach to personal data processing. Companies whose image has suffered in the past as a result of insufficient data protection provided to customers now have an opportunity to rebuild their credibility. Businesses in the tourism industry will need to prove that they are processing their customers' personal data in compliance with the law, as well as demonstrate this fact before the supervisory authority in accordance with the accountability principle. This can be done, for example, by obtaining certification.

The implementation of data protection mechanisms makes it possible to respond to issues more quickly. This is another benefit offered by the implementation of the new regulations. Each organisation that processes personal data will be obligated to implement appropriate technical and organisational measures. In doing so, it will also need to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons. In conclusion, organisations will be obligated to analyse risks in order to react to crisis situations as quickly as possible.

Literature

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union*. L 119, 4 May 2016.

[2] Polish Data Protection Act of 10 May 2018. *Journal of Laws*. 2018, item 1000.

[3] KRASUSKI, A.: *Ochrona danych osobowych na podstawie RODO*. Wolters Kluwer, Warsaw, 2018.

[4] FELIŃSKI, J.: *Ochrona danych osobowych w oświacie*. Wolters Kluwer, Warsaw 2018.

[5] RZETELNA GRUPA Sp. z o.o.: *Pierwsza w Polsce kara za naruszenie przepisów RODO - milion złotych*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://www.politykabezpieczenstwa.pl/pl/a/pierwsza-w-polsce-kara-za-naruszenie-przepisow-rodo-milion-zlotych

[6] ODO 24: *Umowa powierzenia przetwarzania danych osobowych zgodna z RODO – udostępniamy gotowy wzór*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://odo24.pl/blog-post.wzor-umowy-powierzenia-przetwarzania-danych-zgodny-z-rodo

[7] OnlineGDS: *GDS for Hotels*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://www.onlinegds.com/

[8] MerlinX: *System rezerwacyjny*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://www.merlinx.pl/

[9] MINISTERSTWO ROZWOJU: *CEIDG*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://prod.ceidg.gov.pl/ceidg/ceidg.public.ui/search.aspx

[10] PBSG: *RODO statystyki*. [online]. 2019 [accessed 2019-04-22]. Available from WWW: https://www.pbsg.pl/rodo-statystyki

OBECNÁ REGULACE OCHRANY ÚDAJŮ: PŘÍLEŽITOSTI A RIZIKA PROVÁDĚNÍ GDPR V CESTOVNÍM RUCHU

Článek se pokouší odpovědět na nejčastější dotazy týkající se zpracování osobních údajů v cestovním ruchu. Jedná se o pokus vysvětlit základní definice ochrany osobních údajů. Doporučuje se, aby organizátoři, touroperátoři a majitelé hotelů a penzionů byli spokojeni tak, aby zpracování údajů fyzických osob bylo v souladu s GDPR. Rovněž se doporučuje ohrozit zpracování osobních údajů a možnosti, které zajistí bezpečnost údajů zpracovávaných poskytovateli služeb z odvětví cestovního ruchu.

DATENSCHUTZ-GRUNDVERORDNUNG: CHANCEN UND RISIKEN DER UMSETZUNG DER DSGVO IM TOURISMUS

Der Artikel ist ein Versuch, die am häufigsten gestellten Fragen zur Verarbeitung personenbezogener Daten in der Tourismusbranche zu beantworten. Es wird versucht, die grundlegenden Definitionen zum Schutz personenbezogener Daten zu erläutern. Es wird empfohlen, dass die Veranstalter, Reiseveranstalter und Eigentümer von Hotels und Pensionen zufrieden sind, damit die Verarbeitung von Daten natürlicher Personen im Einklang mit der DSGVO steht. Es wird auch empfohlen, die Verarbeitung personenbezogener Daten und die Wahrscheinlichkeiten zu bedrohen, die die Sicherheit der von Dienstleistern der Tourismusbranche verarbeiteten Daten gewährleisten

OGÓLNE UREGULOWANIA OCHRONY DANYCH: SZANSE I ZAGROŻENIA WDRAŻANIA RODO W TURYSTYCE

Artykuł stanowi próbę odpowiedzi na najczęściej pojawiające się pytania w zakresie przetwarzania danych osobowych w branży turystycznej. Jest próbą wyjaśnienia podstawowych definicji dotyczących ochrony danych osobowych. Wskazane są obowiązki, które powinny być spełnione przez organizatorów, touroperatorów czy właścicieli hoteli i pensjonatów by przetwarzanie danych osób fizycznych było zgodne z RODO. Wskazane są również zagrożenia w przetwarzaniu danych osobowych oraz szanse, które pozwolą zapewnić bezpieczeństwo danych przetwarzanych przez usługodawców z branży turystycznej.