

GDPR AND TOURISM: LEGAL FRAMEWORK, COMPLIANCE AND IMPLICATIONS FOR THE TOURISM INDUSTRY

Ioanna C. Chatzopoulou

Department of Tourism Management, University of Patras, Greece

Abstract

This article presents the EU's data protection legislation and guidelines that companies should follow in order to be GDPR compliant and avoid costly fines.

Furthermore the article examines how the new data protection regulation affects tourism businesses (hotels, caterers, travel agencies, etc.), which gather, process and work with users', employees and suppliers personal and sensitive data. There are also mentioned notable cases, where fines were imposed in companies from tourism sector because they violated GDPR.

In Greece but also abroad, where tourism is a very profitable financial activity, compliance with the new regulatory framework for personal data law is crucial for all stakeholders as it depends on the proper functioning of each tourism business and could offer an opportunity to build trustful relationships with customers.

Keywords: *GDPR, legal framework, personal data, tourism, penalties*

1. INTRODUCTION

In information technology the term data refers to anything that can be measured or stored. Data are distinct from information and information can be produced from data through processing. The term data processing includes collecting, cleaning, structuring, storing, accessing, analysing, combining, communicating, restricting or deleting the data. In legal terms though, there is a special category of data that are called personal data. "Personal data is any information that relates to an identified or identifiable living individual" [1]. The living individual whose data are processed is called data subject. In addition personal data are considered different pieces of information that, when put together, can lead to the identification of a particular person. Personal data are for example a name and surname or an Internet Protocol (IP) address. Moreover examples of sensitive personal data are the racial or ethnic origin of the data subject, his political opinions or his sexual life [3]. On the other hand examples of data that are not considered personal are anonymised data or data of a person that is not alive.

EU has recognised the need to protect data privacy and security of its member countries citizens. It has legislate and imposed very strict regulations. Firms that do not comply with EU personal data legislation face extremely costly fines.

In tourism sector, companies manage customer data when they process business functions such as advertising, booking, payment or record potential interest and launch marketing campaigns. Customer data can vary from an anonymous satisfaction survey to identifiable information like names, email addresses, as well as passport information and biometrics. It should be mentioned that companies manage and process their personal data too.

This article presents the key points of EU legislation for personal data protection and security. It explains why such legislation is necessary especially in tourism industry. Additionally it refers to measures that have to be taken by enterprises in tourism sector in order to be compliant with EU legislation. Finally it focuses on infringements that have occurred and fines that have been imposed.

2. THE NEED FOR DATA PROTECTION

2.1. The value of data

Nowadays data is a valuable asset for any company. Even raw data can offer valuable information in managers. This is possible since algorithms and information techniques have made possible the extraction of information out of raw data. Such techniques are for example:

- AI (Artificial Intelligence) - a branch of computer science that has to do with problem solving using software capable of performing tasks that typically require human intelligence.
- Data mining - a process used to extract usable data and patterns out of a very big set of raw data and
- OLAP (Online Analytical Processing) - performs multidimensional analysis of business data and provides the capability for complex calculations, trend analysis, and sophisticated data modeling.

Many industry experts and popular business publications, have recently attested that data is “the new oil”: Wealth and power can be produced by data analysis and processing. The information that is produced leads to knowledge and better decision making. Especially the possession of personal data can lead to discovery of sensitive information about an individual or the discovery of behavioral characteristics. The ones who possess the data actually possess a precious resource of information. Some well known companies such as Facebook, Yahoo, Google and others have made their fortune based on the data they collect, store and process. Information itself becomes a marketable commodity like never before. This is due both to the production of information itself and to the ease with which it is stored and distributed.

The true value of data can therefore only be unlocked if it is shared and re-used.

However, data must have a number of properties, in order to be usable, such as:

- 1) They must be clean and accurate. They should not contain garbage e.g. the data obtained from a customer must not contain incorrect or invalid values. Also the data must express exactly the entity to which they correspond.
- 2) They must be complete. This means that they must include all the parts of which they are composed (eg a person's name must have at least both a first name and a second name).
- 3) They must be authentic. Corrupted data are dangerous. They can lead to wrong decisions or create serious risks.
- 4) They must be in proper form. Data often has a strictly structured format defined by their storage and management software (eg a database management system). However most of the data are either in semi-structured format (highlighter language files, xml, html, tex) or unstructured (text files). The predefined formats that data can take are called formats. There are a number of data encoding formats by type. Indicatively for text data we can mention formats such as pdf, doc, docx, txt).
- 5) They must be accessible. The data must be accessible when users need it. That is, the data must be available at the time there are requested. In addition, data storage and transfer technologies must guarantee their safe access by users.
- 6) They must be up to date. This means that the data must be valid in relation to their reference time.

We must also keep in mind that data are not static entities. On the contrary, data are dynamic and transferable entities. In contrast to a real estate asset of a business eg a building, data can be transferred from one information system to another. Or they may need to change their format or organization in order to achieve goals such as data sharing or redundancy, or the interoperability of applications.

So it is extremely important how to handle data. It is also important to keep data safe and protected. Moreover, legal issues (who has the right to manage the data) and ethical issues (how the information is used) arise.

2.2. Why the need for the data protection?

Obviously data need protection like any other valuable asset. In recent years there were cases where data breaches and scandals appeared due to defective security measures. The legal framework for the treatment of personal data, before 2018, was not firm, uniform and clear. This has been recognised in Europe. In Europe, privacy and data protection are considered vital components for a sustainable democracy. EU designed a new legal framework to safeguard personal data. This framework clearly states that personal data of an individual belong to him and not to the company that keeps or processes them. According to this legal framework high fines can be imposed on companies not complying with the obligations under the Regulation.

3. WHAT IS GDPR

3.1. GDPR framework

GDPR is the acronym of General Data Protection Regulation. Actually it is a EU regulation that supersedes the Data Protection Directive 95/46/EC. It was adopted on 14 April 2016 (2016/679) and put into effect on May 25, 2018. Although it is directly binding and applicable there may be differences in how certain aspects of the regulation are interpreted and enforced in different member countries. GDPR is a EU law that handles data privacy and security matters across all of its members countries in a uniform and strict way. It imposes obligations onto organizations not only in EU but worldwide. The Regulation strengthens existing citizens' rights, provides for new rights and gives citizens of EU more control over their personal data [1].

GDPR recognizes that any data subject as an individual owns privacy rights that have to be respected by anyone who keeps personal data. In the following list are summarized data subjects' privacy rights [9]:

- The right of access to their data
- The right to be informed on how that data is processed and ensuring that that information is available in a clear and understandable way
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling [1].

The GDPR 2016 consists of eleven chapters and every chapter comprises of a set of Articles. In the following paragraphs key regulatory points of the GDPR are presented.

3.2. Data protection principles

Article 5 provides six protection and accountability principles relating to processing of personal data. In particular:

“Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);*

- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');*
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- (d) accurate and, where necessary, kept up to date; According to the Regulation every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');*
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"* (Article 5 , par. 1).

A company must not only be GDPR compliant but must also be able to demonstrate its compliance. Otherwise it is considered that it is not GDPR compliant. It is vital, appropriate technical and organisational measures to be taken in advance to ensure that processing is performed in accordance with the Regulation. Those measures shall be reviewed and updated where necessary (GDPR, Article 24).

The following measures, among others, support a company's GDPR accountability:

- The staff must be aware of their data protection responsibilities.
- The staff must be trained to follow procedures to keep data safe and secure.
- An expert have to be appointed as Data Protection Officer (DPO).
- In case that data processing outsourcing takes place, then an agreement must be signed between company and the third party.
- Records for the data must be kept. That is information about the data such as how the data are used, where they are stored, who is responsible for them.

Not every company needs a DPO. GDPR Article 37 defines three cases where a DPO is required.

- The processing is carried out by a public authority or body, other than a court acting in a judicial capacity.
- The core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- The core activities consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

Of course a DPO can be designated even if a company is not required to do so. A DPO can be a member of company's staff or not. A DPO acts as a contact person for the regulatory authority. In addition a DPO advises and trains company's staff on how GDPR applies. Also a DPO contacts audits and monitors GDPR compliance [1].

Data security means that confidentiality and integrity of data is assured though their availability to company's processing system is not compromised. This can be achieved with techniques such as data encryption or pseudonymisation, that render data useless to an attacker. Moreover a security risk analysis can take place regularly so that the effectiveness of security measures to be assessed. Considering the security outcomes new security measures are planned. Other information security policies such as two factor authentication or backup and restore service can also be implemented. With

these measures the restoration of data will be precise and fast in case of a physical or technical incident.

According to GDPR Article 6 the processing of personal data is illegal unless it can be justified. In the following cases processing of subject data is justified.

- (1) The data subject has given for one or more processing activities, unambiguous consent to process his data. The permission must be freely given, clear, and easy to withdraw.
- (2) The data processing activity is necessary to execute or to enter into a contract to which the data subject is a party.
- (3) Legitimate interest is used as a legal basis for data processing. That is processing is necessary for compliance of a company with a legal obligation.
- (4) The vital interests of the data subject have to be protected through data processing. This can take place in emergency and medical care situations.
- (5) A data processing activity has to take place on behalf of a government entity.
- (6) Processing is necessary for the purposes of a legal obligation.

Finally the legal basis for data processing needs to be documented and the data subject to be informed. Additionally in case of change in the legal basis the data subject has to be notified. In case of data leak, the data subjects must be informed in 72 hours. Otherwise a company will face penalties.

According to GDPR Article 25, protection of personal data has a central role in a company. In their whole life cycle data must be protected. This means that the concept of “data protection by design and by default” will apply in any data processing stage. This concept is well known as ‘privacy by design’ [4] and can be described by the following seven guidelines:

- (1) Proactive not Reactive/Preventative not Remedial. It is better to prevent a security leak than to cure security breach
- (2) Privacy as the Default. Privacy needs to be at the first priority for anything a company does.
- (3) Privacy Embedded into Design. The design of a service or a product must be designed in such a way that no security vulnerability exists.
- (4) Full Functionality. Functionality must not be compromised in favor of privacy.
- (5) End-to-End Security. The data must be safeguarded throughout their whole life cycle.
- (6) Visibility and Transparency. Data subjects should know about privacy mechanisms a company uses to process their data.
- (7) Respect for User Privacy. A data subject can grant or withdraw their consent for processing their data. The data belong to data subject and not to any company.

The concept of consent is defined in Article 4(11) as: “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Article 7 also sets out further ‘conditions’ for consent, with specific provisions on:

- keeping documentary evidence to demonstrate consent;
- clearness and assertivity of consent requests;
- the right to withdraw previously given consent whenever the data subjects want [8];
- freely given consent if the processing of personal data is necessary for the performance of a conditional contract.

GDPR affects almost every tour operator, or travel agency around the world. If a travel agency has customers that are EU citizens has to comply with GDPR. Even if it does not work with EU

destinations but has customers who are EU citizens, it needs to comply with GDPR. Personal data that belong to EU citizens must be protected to a level deemed safe under the new legislation.

Hotels and the intermediary online services must also keep their customers' personal data safe and secure. The data have to be retained for a minimum of one year. In any case that the data are going to be used for any purpose different than visitor registration clear consent must be requested and given.

4. WHAT SHOULD THE COMPANIES DO IN ORDER TO BE GDPR COMPLIANT

In the following specific directions are given that help companies to comply with GDPR. These directions help companies "not only to keep secure and protect their customers' data but also to avoid costly fines for non-compliance" [6].

A company has to be able to prove that keeps data on lawful and transparent basis. This means that a company must be able to present what kind of data it holds and processes and also which are the sources of that data. Moreover a company must be able to prove which has access to the data and how long will the data be kept. It also must justify the reason it keeps and processes personal data. In addition people must be informed that their data are collected and why.

A company must pay special attention to the data it holds in their whole life cycle. According to Article 25 GDPR "The principles of data protection by design and by default" have to be followed. Organizational and technical measures must be taken even before the processing of data. Such technical measures are data encryption, pseudonimization or anonymization. Organizational measures are for example data awareness for all company staff, data protection impact assessment or in case of data breach, the existence of a process to notify authorities.

The Regulation requires in specific cases the designation of a person, entitled data protection officer (DPO), who is responsible for company's compliance with GDPR and also for data governance (Article 37). In case that outsourcing of company's data takes place, then an agreement must be signed between company and the third party, so that GDPR compliance is guaranteed. Even companies that not belong to a EU member country but process personal data of EU citizens are obliged to comply with GDPR regulation [7].

A company must be aware for the privacy rights of its subjects of personal data. Company must be able to report what personal data keeps about them, how long is going to keep them and how the data are used. Company must be able to update, stop processing, transfer to another company or even delete their data from company's files upon request. More over in case of machine decision making all rights and legitimate interests of personal data subjects must be protected.

5. GDPR FINES AND COMPENSATIONS

GDPR articles 83 and 84 define the general conditions for imposing administrative fines and penalties. Companies that do not comply with GDPR can face costly financial penalties. The amount of the fine depends on the infringement and the firm. Additionally, according to Article 82 data subjects have the right to ask for compensation from companies that cause them material or non-material damage as a result of a GDPR non compliance.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year. The GDPR fine would be the maximum fine applicable for your company whichever amount is higher. Fines up to €20 million or 4% of annual global revenue can be claimed, whichever amounts to highest value.

The GDPR authorizes the national data protection agencies to be the chief enforcing bodies of the law in each EU country. The European Data Protection Board (EDPB) is the lead supervising body of the GDPR. This body is comprised of representatives from each national data protection authority.

The fines differentiate based on the what articles of the GDPR a company violates: if it violates its own obligations it will be subject to lower level fines, whereas violations of individual privacy rights will be subject to higher level fines. Authorities in each EU country determine whether a fine will be assessed and in what amount according to the following 10 criteria [10]:

- What was the gravity and nature and duration of the infringement. That is what was the nature of the infringement, how much people were affected, what damage they suffered and for how long?
- The infringement was intentional or or due to negligence?
- Did the company take measures to mitigate the damage happened due to infringement?
- How much was the company prepared to comply with GDPR?
- What is the history of company's previous infringements under the Data Protection Directive and GDPR?
- Did the company coopare with authorities to discover and remedy the infringement?
- What categories of personal data were affected by the infringement?
- Did the infringement was reported to the supervisory authority?
- Did the company adherence to certified industry standards?
- What other issues were arised from circumstances of the infringement?

Fines are imposed on companies and businesses who violate the GDPR. There are several databases that give an overview of fines and penalties, which data protection authorities within the EU and UK have imposed under the EU GDPR. Examining them we can notice that fines are imposed on companies of any sector and of any size.

In the following figures are presented statistics based on PrivacyAffairs.com [5], last updated on 7 June 2021.



Fig. 1. Statistics on GDPR fines

Source: <<https://www.privacyaffairs.com/gdpr-fines/>>

5 MOST RECENT GDPR FINES

*Only includes finalised cases

DATE	ORG	FINE
06/02/2021	Avalos Consultores, S.L.	€4,000
05/27/2021	Private individual	€2,000
05/25/2021	Desolasol Restauracion, S.L.	€6,000
05/25/2021	Alava Norte, S.L.	€4,000
05/25/2021	Vodafone Espana, SAU	€100,000

Fig. 2. Five more recent GDPR fines

Source: <<https://www.privacyaffairs.com/gdpr-fines/>>

TOP 5 BIGGEST GDPR FINES

*Only includes final & binding fines

 Google Inc.	€50,000,000
 H&M Hennes & Mauritz Online Shop A.B. & Co. KG	€32,258,708
 TIM - Telecom Provider	€27,800,000
 British Airways	€22,046,000
 Marriott International, Inc	€20,450,000

Fig. 3. Top five biggest GDPR fines

Source: <<https://www.privacyaffairs.com/gdpr-fines/>>

Marriot international, Inc case: A fine of €20,450,000 was imposed on the company due to violation of article 32 GDPR. The type of infringement was “failure to implement sufficient measures to ensure information security”. “In a cyber incident previously notified to the information commissioner (ICO) on November 18, Marriott International unintentionally exposed the personal data of over 330 million guest records globally, out of which 30 million were residents of 31 countries in the European Economic Area.” [5]

British Airways case: The company has to pay a fine of €22,046,000 due to violation of articles 5 GDPR and 32 GDPR. The type of infringement was failure to implement sufficient technical and organizational measures to ensure information security. The breach notified in 2018 by British Airways and affected both personal and credit card data. The data harvested included log in information, credit card and travel booking details as well name and address information. The official website of the British Airways was diverted to a fraudulent website. This scammers would steal the customer details of all clients taken there. It is estimated that the personal data of more than 500,000 customers were stolen during the incident.

6. CONCLUSIONS

Personal data are both valuable and sensitive. That is why EU has imposed a new legal framework that is called GDPR. The GDPR was enforced from May 25 2018 to every member state, and till now it is in place. It shields the rights of data subjects and imposes high financial penalties to those companies that do not comply with it. Companies have to re-examine their strategy towards personal data handling and take organisational and technical measures in order to comply with GDPR.

REFERENCES

1. 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) Official Journal L. 2016 ;119, 4 May 2016.
2. GDPR checklist for data controllers, viewed 22 June 2021, <<https://gdpr.eu/checklist/>>.
3. What is personal data? viewed 22 June 2021, <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>

4. Nicole, O. "Implementing Privacy By Design", viewed 15 June 2021, <<https://www.privacypolicies.com/blog/privacy-by-design/>>.
5. GDPR Fines Tracker & Statistics, viewed 26 June 2021, <<https://www.privacyaffairs.com/gdpr-fines/>>.
6. Veale, Michael; Binns, Reuben; Ausloos, Jef (2018). "When data protection by design and data subject rights clash". *International Data Privacy Law*. 8 (2): 105–123. doi:10.1093/idpl/ipy002.
7. Alice, Baker (18 January 2018). "How to transfer data to a 'third country' under the GDPR", viewed 5 May 2021 <<https://www.itgovernance.eu/blog/en/how-to-transfer-data-to-a-third-country-under-the-gdpr>>
8. S Kulk and FJ Zuiderveen Borgesius, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in J Polonetsky, O Tene, and E Selinger (eds) *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2018).
9. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law*, 28:1, 65-98, DOI:10.1080/13600834.2019.1573501
10. What are the GDPR Fines? viewed 2 June 2021, < <https://gdpr.eu/fines/>>.