Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Diploma Thesis

General Data Protection Regulation in the European Union and its application and impact on business

Author: Oleh Popov

Supervisor: Ing. Miloš Ulman, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Oleh Popov

European Agrarian Diplomacy

Thesis title

General Data Protection Regulation in the European Union and its application and impact on business

---

Objectives of thesis

The thesis is intended to study GDPR implementation in the European Union. The main objective of the research is to describe the mechanism of application of the GDPR in a selected business, examine its impact on the conducting of business activities, identify shortcomings and advantages.

Partial goals of the thesis are such as:

- To create the literature review of the GDPR in the European Union.

- To study controversial issues for GDPR.

- To develop a case study of GDPR application in the given organization to evaluate its impact on business activities.

Methodology

Methodology of this thesis consists of two major approaches: literature and legislation review, and empirical research. The theoretical framework of the research will be outlined by the literature and legislation review. The practical part will consist of a case study of the given organization and its implementation of GDPR. The GAP analysis and dataset mapping will be used to collect primary data. Received data will be collected processed and interpreted with appropriate analytical methods resulting in a proposal of steps to ensure organization's compliance with GDPR. Main findings will be generalized and used for final conclusions.

The proposed extent of the thesis

60 – 80 pages

Keywords

GDPR, GAP analysis, Data Protection Officer, DPIA, hospitality.

Recommended information sources

Blackmer, W.S. (5 May 2016). GDPR: Getting Ready for the New EU General Data Protection Regulation. Information Law Group. http://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R. & Schiffner, S., (2015). Privacy and Data Protection by Design-from policy to engineering, https://arxiv.org/abs/1501.03726

European Commission. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

Georgiev, Georgi. GDPR Compliance Cost Calculator. GIGAcalculator.com. https://www.gigacalculator.com/calculators/gdpr-compliance-cost-calculator.php

How Smart Businesses Can Avoid GDPR Penalties When Recording Calls. xewave.io. https://www.xewave.io/how-smart-businesses-can-avoid-gdpr-penalties-when-recording-calls/

Tarhonen, Laura (2017). Pseudonymisation of Personal Data According to the General Data Protection Regulation. https://www.edilex.fi/viestintaoikeus/18073

Expected date of thesis defence

2018/19 SS – FEM

The Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 30. 10. 2017

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 1. 11. 2017

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 25. 02. 2019

Declaration

I declare that I have worked on my diploma thesis titled "General Data Protection Regulation in the European Union and its application and impact on business" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 11.03.2019

Oleh Popov

Acknowledgement

I would like to thank to my supervisor Ing. Miloš Ulman, Ph.D. for his tremendous contribution and invaluable help in preparing this thesis.

Furthermore, I would like to thank Petr Sobotka for his support and professionalism, as well as my girlfriend, which inspired and supported me throughout studies

General Data Protection Regulation in the European Union and its application and impact on business

Abstract

This thesis was written in order to assess the impact of the introduction of the GDPR on business activities. It includes work with legislation and literature, as well as practical research on the example of the hotel.

Within the theoretical part, the background to the introduction of the GDPR in the European Union, as well as the main innovations of this law in the context of the rights and obligations of the parties were studied. In addition, the main controversial issues of the GDPR in relation to modern technologies, business and ordinary citizens were outlined, and potential consequences were identified.

The practical part deals with the GDPR implementation in the hotel, it's risk assessment and costing. The impact of the GDPR on income, expenses, number of guests and the level of hotel service was analyzed. The results obtained were compared with the GDPR implementation project's outcome from other hotels.

The conclusion summarizes results of theoretical and practical parts, emphasizing and generalizing the main findings of the research.

Keywords: GDPR, GAP Analysis, Data Protection Officer, DPIA, hospitality, compliance, consent, Records of Processing Activities, Data Protection, privacy.

Obecné nařízení o ochraně údajů v Evropské unii, její uplatňování a vliv na podnikání

Abstrakt

Tato práce byla napsána za účelem posouzení vlivu ONOOÚ na podnikatelskou činnost. Zahrnuje práci s legislativou a literaturou, stejně jako praktický výzkum na příkladu hotelu. V rámci teoretické části byly studovány předpoklady o zavedení ONOOÚ do Evropské unie, jakož i hlavní inovace tohoto zákona v kontextu práv a povinností stran. Kromě toho byly identifikovány hlavní kontroverzní otázky ONOOÚ týkající se moderních technologií, podniků a obyčejných občanů a byly zjištěny potenciální důsledky.

Praktická část je věnována realizaci ONOOÚ v hotelu, hodnocení rizik a nákladů. Byl analyzován vliv ONOOÚ na příjmy, výdaje, počet hostů a úroveň hotelových služeb. Získané výsledky byly porovnány s výsledky realizace projektu ONOOÚ v jinych hotelech.

V závěru jsou shrnuty výsledky teoretické a praktické části, hlavní závěry výzkumu jsou zdůrazněny a rekapitulovany.

Klíčová slova: ONOOÚ, GAP analýza, pověřenec pro ochranu osobních údajů, DPIA, pohostinstvi, soulad, souhlas, záznamy o zpracovatelských činnostech, ochrana dat, důvěrnost.

Table of content

List of tables

List of figures

List of abbreviations

GDPR – General Data Protection Regulation;

EDPS – European Data Protection Supervisor;

EU – European Union;

OECD – Organization for Economic Co-operation and Development;

DPO – Data Protection Officer;

CIPL – Centre for Information Policy Leadership;

DPIA – Data Protection Impact Assessment.

1 Introduction

Recently, the problem of data protection has become one of the most burning and debated, so the issue of protecting personal data has become more urgent than ever. We owe this to the continuous and very rapid growth of modern technologies, which are becoming more and more common in our lives. One of the tools to limit the impact of technology on personal data was the adoption of the General Data Protection Regulation in May 2018, which is designed to address current challenges in the field of personal data protection and unify personal data protection in the European Union.

It is difficult to overestimate the role of data protection in modern society, since each person using the services or buying goods leaves a trace of his/her personal data. It can be a name, nationality, date of birth, religious beliefs, and some data can be very fragile and that their theft or possible misuse by the individual could be very detrimental. This work has a clear focus on the study of the General Data Protection Regulation, which is designed to significantly and qualitatively improve the level of personal data protection.

The theoretical part of this work focuses on the origins of personal data protection in the European Community, describing the forerunners of modern legislation and its evolution, as well as the reasons for the transition to the General Data Protection Regulation. In addition, this work considers the General Data Protection Regulation itself, giving a brief description of the basic concepts, determining the territorial scope, identifying the basic rights and duties of individuals and entities falling under this law and emphasizes the main points of contention of the General Data Protection Regulation in various fields of activity.

The practical part is aimed at the implementation of the General Data Protection Regulation in a selected company, and reveals the main characteristics, portfolio of services, as well as the main indicators of economic activity. An analysis of the current system of personal data protection has been carried out, which found inconsistencies with the General Data Protection Regulation. Based on the established inconsistencies, a GDPR implementation schedule was developed, and remedial steps were proposed and implemented to achieve the company's full compliance with all General Data Protection Regulation rules and provisions.

In the final part, a cost estimate for the implementation of the General Data Protection Regulation at the enterprise was made, and the risks and effects on the economic activity were assessed.

2 Objectives and Methodology

2.1 Objectives

The thesis is intended to study GDPR implementation in the European Union. The main objective of the research is to describe the mechanism of application of GDPR in a selected business, examine its impact on the conducting of business activities, identify shortcomings and advantages.

Partial goals of the thesis are such as:

- To create the literature review of GDPR in the European Union. To consider the European legislation in the field of data protection, which preceded the introduction of GDPR, to explore the main reasons for the transition to the new legislation, as well as delve into the main innovations of the GDPR and the rights and obligations of parties.
- To study controversial issues for GDPR. To identify the main areas of influence of the GDPR on business and ordinary citizens, as well as examine and analyze its potential consequences.
- To develop a case study of GDPR application in the given organization to evaluate its impact on business activities. To create a step-by-step plan for the implementation of the GDPR, taking into account the specifics of the company, apply it, assessing the real consequences on the level of service, income, expenses and number of guests, compare the results with similar businesses. To conduct cost calculation and risk assessment.

2.2 Methodology

Methodology of this thesis consists of two major approaches: literature and legislation review, and empirical research. The theoretical framework of the research will be outlined by the literature and legislation review. The practical part will consist of a case study of the given organization and its implementation of GDPR. The GAP analysis and data mapping will be used to collect primary data, received data will be collected processed and interpreted with appropriate analytical methods resulting in a proposal of steps to ensure organization’s compliance with GDPR. Critical Path Method will be used for scheduling

GDPR implementation activities, and the risk assessment approach developed by the Centre for Information Policy Leadership (Hunton & Williams LLP) will be applied to evaluate the GDPR implementation project's risk. Main findings will be generalized and used for final conclusions.

2.3 Importance of the Study

As technology grows, the importance of protecting personal data increases. The introduction of the GDPR leads to the need to meet its requirements, first of all it applies to business. The study of the main provisions of the GDPR, as well as the development of a project for its application, will be an excellent practical tool for application of its norms and provisions in any business.

3 Literature Review

This section includes the study of articles, books, research and laws that the author deemed necessary for writing this section.

3.1 Legal background of the General Data Protection Regulation

One of the key points of this work is business compliance with the basic rules and regulations of the GDPR, as well as the challenges and difficulties that the business may face. Therefore, in the context of this work, it is very important to study and understand what is considered a legitimate basis for data protection and privacy law. That is why this chapter contains a description of the most important documents and development stages that led to the introduction of GDPR in the EU. In addition, in this chapter we will touch upon the main reasons and motivations for repealing the old legislation and introducing GDPR.

3.1.1 European Convention on Human Rights

In the context of Europe and the European Union, the concept of personal data and its protection became relevant in the post-war period, when the Universal Declaration of Human Rights (1948) was adopted. Declaration listed a right to privacy as one of the fundamental human rights.

Over time, the concept of the right to privacy was expanded in the European Convention on Human Rights. (1950)

Key concepts are described in “Article 8 – Right to respect for private and family life”:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (European Court of Human Rights, 1950).

Thus, this document regulates non-interference in the personal life of a person, both of another person and of state bodies. Moreover, in the context of this article, the European Court of Human Rights issued several decisions on the regulation of personal data by business companies, in particular, illegal storage of personal data, misusing of data, etc (Woods, 2015).

3.1.2 Data Protection Convention

With the growth of information technology, already in 1980, the OECD issues recommendations on data protection, and in 1981 the Council of Europe adopts the Data Protection Convention (Treaty 108).

The convention was agreed on January 28, 1981 by the Council of Europe and entered into force on October 1, 1985.

In accordance with the agreement, the signatories wanted to ensure data protection under the Convention. Considering the increase in cross-border data traffic, signatory came to solution that a single level of data protection should be established. However, it was also noted that excessive data protection may impede the exchange of information between individual states.

A key aspect of this convention was the rights and freedoms of people residing in the territories of the subscribing countries. In particular, this concerned the right for privacy of people as well as the protection of personal data in automated processing.

The Convention includes some elementary principles of confidentiality that have been incorporated into national legislation, including the principle of fair processing of data, the principle of purpose, the principle of necessity and the requirements of information of the person concerned. However, these principles apply only to personal data that is processed automatically. Personal data that is processed only manually - for example, employee data in personal files - is not subject to the European Data Protection Convention.

In addition, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know which information is stored about him or her and have a possibility to access and correct it. (Council of Europe, 1981)

3.1.3 European Data Protection Directive

However, the main achievement in the field of personal data protection was the release of the European Data Protection Directive (1995) which until recently was the main document regulating privacy in the European Union. This document was created taking into account all the new technological changes that have occurred in previous years. Given this fact, we must dwell upon the description of this document.

Data Protection Directive is an EU regulation that is designed to protect the confidentiality and all personal data of EU citizens. This document concerns the collection, processing and use of personal data.

This document is based on the recommendations provided by OECD, which were summarized in several basic principles:

- The person whose data is being collected must be warned about data collection;
- If data is collected, it should be kept safe from abusive use, loss or theft;
- Personal data should not be disclosed or shared with third parties, without the consent of the subject;
- Subjects whose personal data is being collected should be informed as to the party or parties collecting such data;
- Subjects should have granted access to their personal data and be allowed to correct any inaccuracies;
- Data collected should be used only for stated purpose(s);
- Subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles. (Rouse, 2008)

It consists of 34 articles, each of which corresponds to a specific section of personal data protection. In fact, this is the first document in the EU that covered such a wide range of regulation, from data collection to transmission. It was created to tie together already existing legislation in EU member states regarding the protection of personal data, to improve and harmonize it. In addition, the secondary goal was to eliminate restrictions on the movement of information within the EU.

As mentioned above, the Directive applies to both private individuals and public authorities. The provisions imply significant restrictions for the authorities that process the data, at the same time expanding the powers of the data subjects.

This law also has provisions limiting the transfer of personal data abroad. The provisions of the law ensure that the receiving party undertakes to provide a sufficient level of personal data protection.

It should be noted that at the time of creation, this secondary law was innovative. Considering the level of development of technologies and data processing methods, it was relatively easy to create special regulations for each person involved in the processing of personal data. This implies the introduction of restrictions for people responsible for data processing and binding of different procedures to certain operations. However, this document did not set a goal to predict future changes in technologies and to comply with them, but unconditionally became the basis for the new legislation both in Europe and in non-European countries (Neil Robinson, 2009).

3.2 Reasons for moving to GDPR

This chapter examines the main reasons for the adoption of new legislation in the field of personal data protection, namely:

- The failure to adapt to future changes in technology.

  As indicated above, the GDPR did not set the goal to consider changes in technology but was created to regulate existing problems. Speaking about the development of technologies, we can notice that from the end of the nineties to the present-day, mobile phones, computers and other information processing tools have become an integral part of business and society. Given this, the Directive ran into problems that did not even exist before, and as technology grew, the gap between law and technology grew as well. This gap could only be bridged with new legislation.

- The need to enhance data protection in the domestic market.

  One of the main problems faced by transnational firms was the lack of uniform legislation in the field of personal data, despite the general EU policy in this direction. The EU faced with the need to make legislation clearer and more transparent, ensuring compliance and control at all levels.

- The need to reckon with globalization, and as a result, improve international data transfers.

There were several problems in the field of data processing outside the EU, since very often outsourcing was used for this kind of work. There was ambiguity around legislative regulation and responsibility of data handlers. In addition, existing data transmission schemes required substantial improvements to make them easier and less burdensome.

- The need to improve institutional interactions.
  There was a need to improve performance of supervisory bodies as well as giving them new powers to strengthen their role in data protection regulation.
- The need to improve the coherence of the data protection legal framework
  There was a necessity to develop a single tool that would be applied in all sectors of the European Union's data processing policies. In addition, it was necessary to ensure the normal operation and an integrated approach to the personal data protection (European Commission, 2010).

3.3 General Data Protection Regulation

3.3.1 From the European Data Protection Directive to GDPR

As mentioned above, the basics of modern data protection policy were laid down by the European Data Protection Directive, however, more than 20 years passed between the adoption of GDPR and the Directive. Work on the creation of GDPR began in the middle of 2011, when the EDPS Opinion on EC Communication 'A comprehensive approach on personal data protection in EU' was released. This document outlined the main obstacles and challenges facing European policy on data protection, marked the main goals and perspective directions for improving the existing policy. EDPS Opinion was the impetus for the development of EU policies towards the formation and adoption of GDPR. On 07.03.2012, the European Commission proposed to reform European Data Protection Directive, to strengthen online privacy rights and stimulate the EU digital economy development. This initiative has been approved by The European Data Protection Supervisor and Article 29 Working Party with the minor changes and inputs from their sides. And finally, 17.12.2015 Parliament voted for adoption of GDPR, which came into force on 25.05.2018 (European Data Protection Supervisor, 2018).

3.3.2 Definition and principles

The General Data Protection Regulation (GDPR) is a European Union regulation aimed to strengthen and unify the protection of personal data of the European Union citizens. GDPR is intended to give citizens control over their own personal data, and to simplify regulatory framework for international economic relations by unifying regulation within the EU. GDPR has a direct effect in the Member States without the need to implement its provisions at the level of national legislation.

GDPR is based on following principles:

- Legality, fairness and transparency. There must be a legal basis for collection and usage of personal data, non-violation of any laws, openness, and honesty from beginning to end about the personal data usage;
- Specific objectives. All specific objectives should be enshrined in the privacy policy and strictly followed;
- Minimization of the data used. It is necessary to use an adequate amount of data to fulfill the goals set.
- Accuracy. Personal data must be accurate and should not be misleading;
- Data storage restriction – do not store data longer than necessary, periodically audit data and delete unused data;
- Integrity and confidentiality– to store data in a safe place and pay sufficient attention to data integrity;

Accountability. It is responsibility for the processing of personal data and implementation of all other principles of GDPR including confidentiality records, protection use, data validation, appointing a data protection officer (DPO) (European Parliament, The Council of the European Union, 2016).

3.3.3 Territorial scope

3.3.3.1 Controllers and processors established in the EU.

“Controller” for the purposes of GDPR means an individual or legal entity, a government body, an agency or other institution that independently or jointly with others determines the purposes and means of processing personal data.

“Processor” means a natural or legal person, a public authority, agency or other institution that processes personal data on behalf of the controller (European Parliament, The Council of the European Union, 2016).

GDPR “applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union”, regardless of where the data processing takes place: in the EU or outside it. Establishment implies the effective and real exercise of activity through "stable arrangements", regardless of their legal forms: it can be a branch or a subsidiary etc. (European Parliament, The Council of the European Union, 2016)

The definition of “establishment” in GDPR corresponds to the definition given by the Court of Justice of the European Union (“EU Court”) in Weltimmo case in 2015 V NAIH (C-230/14). An organization can be “established” when it carries out “any real and effective activity – even a minimal one” through “stable agreements” in the EU. Even the presence of one representative may be sufficient. Thus, Weltimmo was recognized as having an “establishment” in Hungary as a result of using the website in Hungarian, in which real estate in Hungary was advertised, use of a local agent (who was responsible for debt collection and acted as a representative in administrative and court proceedings), as well as using the postal address and bank account for business purposes - despite the fact that Weltimmo was registered in Slovakia (Court of Justice of the European Union, 2015).

3.3.3.2 Organizations not established in the EU, whose activities are aimed at EU citizens.

Such organizations are subjects to the Regulations if they process personal data of EU data subjects:

- Offering them goods or services (without the requirement of payment);
- Monitoring their behavior in the EU.

To offer goods and services, it is not enough to have a website simply available in the EU. It should be obvious that the organization “foresees” that its activities will be focused on personal data subjects in the EU. The accessibility of the website, e-mail address or the use of the language commonly used in the third country where the controller is established are insufficient to establish such factors. However, the use of a language or currency commonly used in one or more Member States with the ability to order goods and services

in such a language, clearly indicates that the controller is intended to provide goods or services to the EU personal data subjects.

“Monitoring” means tracking individual users on the Internet to create profiles, which are used to predict personal preferences, behavior and attitudes. At the same time, GDPR is not applied in the case of the personal data processing by an individual within the framework of “purely personal or household activity (European Parliament, The Council of the European Union, 2016). It touches correspondence, maintenance of address books, social networks and online events held for social and household purposes. However, GDPR applies to controllers and processors who “provide the means for processing” that fall under this exception.

3.3.4 Personal Data

For the purposes of GDPR, “personal data” means any information relating to an identified or identifiable natural person (“data subject”); An identifiable natural person is a person who can be identified directly or indirectly, by referring to an identifier such as: name, identification number, location data, an online identifier or any factor specific to physical, physiological, genetic, mental, economic, cultural or social identity of the individual (European Parliament, The Council of the European Union, 2016).

The preamble to the Regulation emphasizes that certain categories of online data can be classified as personal - online identifiers, device identifiers, cookie identifiers and IP addresses. In October 2016, the EU Court of Justice clarified the status of dynamic IP addresses in the case of Patrick Breuer v. Germany (C-582/14), indicating that an IP address is personal data when it belongs to an Internet provider, but does not represent personal data if it belongs to a party that does not have means that can reasonably be used to identify a person (Privacy and Data Security Practice Group, 2016).

At the same time, personal data subjected to pseudonymization, and can be related to a natural person using additional information, are considered information about the identified natural person.

3.3.5 Representative of a controller or processor not established in the EU

A controller or processor which is not established in the EU is obliged to appoint a representative if it processes personal data of data subjects located in the EU. This applies

to cases where personal data processing activities are related to supply of goods or services or to monitoring data subject behavior.

Exceptions are cases when:

- Processing is not carried out on an ongoing basis;
- Processing is not carried out on a large scale;
- In relation to special categories of personal data or personal data concerning criminal sentences and offenses;
- Processing will not harm rights and freedoms of individuals, taking into account the nature, context, scope and purposes of processing.

The representative has to be located in one of the EU Member States, where the data subject is located. The representative must act on behalf of the controller or processor and any Supervisory Authority must be able to contact him (European Parliament, The Council of the European Union, 2016).

3.3.6 Relationship between the controller and processor

Processing by the processor must be regulated by a contract or a legally binding document in accordance with EU legislation. It should define subject, duration, nature and purposes of processing; type of personal data and categories of data subjects. It should consider specific tasks and duties of the processor in a context of performed processing and risks for rights and freedoms of data subjects (European Parliament, The Council of the European Union, 2016).

The processor must not interact with another processor without a prior or general written permission of the controller. The controller or processor must keep records of processing operations under his responsibility. Each controller and processor must cooperate with the supervisory authority and make these records available upon request for monitoring of processing operations.

The controller and processor must take appropriate technical and organizational measures to ensure a proper level of data safety. They should consider current status, costs of implementation, nature, scope, context and purposes of processing, as well as risks of harm to rights and freedoms of individuals. Safety measures include:

- Pseudonymization and encryption of personal data;

- Ensuring of continued confidentiality, integrity, availability and sustainability of processing systems and services;
- Ability to timely restore access to personal data in a case of a physical or technical incident;
- Regular testing and evaluation of effectiveness of technical and organizational measures to ensure data processing safety;
- The processor is obliged to notify the controller about any violation of personal data as soon as possible. (European Parliament, The Council of the European Union, 2016)

If the processor violates requirements of GDPR by defining purposes and means of processing, the processor is considered as the controller for this processing and bears the corresponding responsibility.

3.3.7 Data Protection Officer

The controller and processor must appoint an official Data Protection Officer if:

- Processing is carried out by a state body or institution (with an exception of courts operating under their authority);
- Main actions of the controller or processor consist of: processing operations which require regular and systematic monitoring of data on a large scale, or large-scale processing of special categories of data and personal data related to criminal records and offenses.

"Regular and systematic monitoring" includes all forms of online monitoring and profiling, including behavioral advertising, redirection of emails, location determination, monitoring of health and physical activity, covert surveillance, processing by connected devices (smart meters, smart cars, etc.), data-based marketing activities (the so-called "Big Data").
Data Protection Officer should have expert knowledge in data protection legislation and practice. A level of expert knowledge is determined in accordance with data processing operations performed and protection required.
The controller or processor should:

- Publish contact details of the DPO and transfer them to a supervisory authority;

- Ensure that the DPO does not receive any instructions on performance of his functions.

Data Protection Officer should perform at least following functions:

- To inform and consult all the people involved in a personal data processing about obligations in accordance with GDPR and other data protection provisions;
- To monitor compliance with GDPR;
- To monitor policy of the controller and processor regarding personal data protection;
- To provide consultations regarding evaluation of the data protection level, and monitor its effectiveness;
- To cooperate with the supervisory authority;
- When it is necessary to act as a contact point for the supervisory authority on issues related to data protection. (European Parliament, The Council of the European Union, 2016)

GDPR allows to assign one DPO to a group of companies, but this person should be easily accessible from each company.

If the DPO is appointed on a voluntary basis, the controller and processor must meet the same requirements which established by GDPR for cases of mandatory appointment.

If appointment of the DPO is not mandatory and the DPO is not appointed voluntarily, other employees or external consultants may be appointed to perform respective functions.

3.3.8 Consent

In some circumstances Directive 95/46 / EC permitted controllers to rely on implicit consent and "refusal" (opt-out), but GDPR established that consent must be given by a clear affirmative action. Consent must be intelligible, specific and informative in a form of written, electronic or oral statement. In accordance with GDPR, an electronic consent may be given in the form of any statement that makes it clear that the subject agrees on processing of his personal data.

Explicit consent should be obtained in the following cases:

- For processing of special categories of personal data (race or ethnicity, political, religious or philosophical beliefs, membership in trade unions, genetic data, biometric and health data);
- To make decisions regarding the data subject "based solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects him or her;
- To transfer personal data to countries that do not provide a sufficient level of protection, unless another transfer mechanism is installed. (European Parliament, The Council of the European Union, 2016)

Consent must cover all types of processing carried out for the same purpose. When processing has several goals, it is necessary to obtain consent for all of them.

The data subject has a right to withdraw his consent any time. Controllers must inform the data subjects about a right of withdrawal before obtaining a consent. After the consent is withdrawn, data subjects have a right to demand the removal of personal data and termination of data processing.

GDPR contains special provisions regarding children's personal data processing. If information society offers services directly to a child, processing of a child's personal data is legal only if he or she is more than 16 years old. For children under 16, consent should be given by parents or a person performing functions of a parent.

3.3.9 Measures of personal data protection

GDPR introduces a concept of "data protection by design". At a conceptual level, data protection by design means that confidentiality should be a distinctive feature at a product development stage, rather than being implemented later.

GDPR establishes a general duty for controllers, to take appropriate technical and organizational measures taking into account "state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." (European Parliament, The Council of the European Union, 2016). It should be taken during determination of means for processing and during processing of personal data itself.

However, unlike Directive 95/46 / EC, GDPR contains specific proposals on what types of security measures can be considered "risk appropriate", including:

- Pseudonymization and encryption of personal data;
- Ability to ensure continued confidentiality, integrity, availability and sustainability of processing systems and services;
- Possibility of timely restoration of access to personal data in a case of a physical or technical incident;
- Regular testing and evaluation of effectiveness of technical and organizational measures to ensure safety of data processing.

The controller must apply appropriate technical and organizational measures to ensure that only personal data which are necessary for each specific processing purpose are processed. This obligation extends to amount of personal data collected, a level of its processing, storage period and availability. In particular, such measures should ensure that personal data are not available to an unlimited number of individuals without human intervention.
GDPR also introduces a notion of "pseudonymization" – "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information (European Parliament, The Council of the European Union, 2016).
Pseudonymization can significantly reduce risks associated with personal data processing, maintaining its usefulness. For this reason, certain provisions of GDPR create incentives for controllers to pseudonymize data collected.

3.3.10 Informing of data subjects

GDPR expands amount of information that the controller must provide to data subjects before collecting personal data. In addition to a name of the controller, purposes of processing and recipients of personal data, controllers should inform data subjects about:

- Data retention period'
- Right to withdraw consent any time;
- Right to request access;
- Right to restrict processing;
- Right to file a complaint to the supervisory authority.

This information should be disclosed in a clear and easily accessible form, using a clear and simple language that is appropriate for relevant audience. However, if the controller

received information not from the data subject, but from another controller or publicly available source, then he does not need to provide this information since it is "Disproportionate effort" (European Parliament, The Council of the European Union, 2016).

If the data subject seeks to exercise one of the rights granted by the Regulation, the controller must take appropriate action without undue delay or no later than one month after the request. However, the controller has the right to extend this period if necessary due to the large number of requests. If the controller does not wish to respond to the request, he must explain his decision to the data subject within one month. All these services should be free of charge, unless requests are manifestly unfounded or excessive.

GDPR provide a right to refuse action on request if the controller demonstrates that he is unable to identify the data subject. On the other hand, if the controller has reasonable doubts about the identity of the person making the request, he may ask him for additional information in order to confirm his identity.

3.3.11 Profiling

GDPR introduces a concept of "profiling" – "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her (European Parliament, The Council of the European Union, 2016).

The data subject must be specifically notified about implementation of profiling and its consequences. The data subject has the right to file an objection to profiling at any time.

3.3.12 Making decisions based on personal data processing

Making decisions based on personal data processing is permissible when:

- This is expressly permitted by legislation of the EU or the Member State which the controller belongs to;
- It is necessary for the conclusion or execution of a contract between the data subject and the controller;
- The data subject gave a consent.

In any case, the controller must ensure that processing is carried out with appropriate guarantees. It includes:

- Provision of specific information to the data subject;
- The right for human participation in decision making;
- The right to express a point of view;
- The right to receive an explanation of the decision made;
- The right to challenge the decision.

3.3.13 Cross-border data transfer

GDPR establishes restrictions on transfer of personal data to "third countries" (i.e., outside the EU) and to international organizations. The transfer of personal data to a third country or international organization can be carried out without permission, if the European Commission decided that a third country or international organization provides an adequate level of personal data protection ("Adequacy decisions") (European Parliament, The Council of the European Union, 2016).

In the absence of a decision on adequacy, the controller or the processor must take measures to compensate the lack of data protection. They must provide appropriate guarantees to the data subject and ensure that effective means of the data subject's rights protection are available, specifically:

- A legal document between the state authorities of the countries;
- Mandatory corporate rules approved by the competent supervisory authority;
- Provisions for standard data protection adopted by the Commission;
- Provisions for standard data protection adopted by the supervisor and approved by the Commission;
- An approved code of conduct;
- An approved certification mechanism.

In the absence of a decision on adequacy, the cross-border transfer of personal data can be carried out only on one of the following conditions:

- The data subject has agreed with the proposed transfer being informed about possible risks due to the lack of a decision on adequacy and appropriate guarantees;
- The transfer is necessary for the contract between the data subject and the controller;

- The transfer is necessary for the conclusion or execution of the contract, which was concluded in the interests of the data subject, between the processor and another natural or legal person;
- The transfer has an important cause and it is carried out in the public interest;
- The transfer is necessary for establishing enforcement and protecting of claims;
- The transfer is necessary to protect vital interests of the data subject if the data subject is physically or legally unable to consent. (European Parliament, The Council of the European Union, 2016)

3.3.14 Data Protection Impact Assessment

The impact assessment for data protection should be carried out by the controller before data processing. This is necessary in order to assess risks to rights and legitimate interests of data subjects, taking into account the nature, extent, context and sources of the risk.
Impact assessment should be carried out in the following cases:

- Personal data are processed to make decisions about specific natural persons after any systematic and extensive assessment of personal aspects related to them;
- Monitoring of public places on a large scale or for any other operations, when the competent supervisor believes that the processing is likely to lead to a high risk for rights and freedoms of data subjects;
- Large-scale processing of a significant amount of personal data at a regional, national or supranational level that can affect a large number of data subjects and lead to high risk for rights and freedoms of data subjects.

Impact assessment at least should include:

- Systematic description of intended processing operations and processing objectives;
- An assessment of the necessity and proportionality of processing operations with respect to objectives of processing;
- Risk assessment for rights and freedoms of data subjects;
- Measures to eliminate risks. (European Parliament, The Council of the European Union, 2016)

3.3.15 Notification about personal data violations

In accordance with GDPR, violation of personal data is a violation of security resulting in "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed" (European Parliament, The Council of the European Union, 2016).

Compared to the Directive 95/46 / EC, GDPR establishes a new notification regime in case of violation of personal data.

The processor is obliged to notify the controller about the violation without undue delay.

The controller is obliged to notify the supervisor about the violation within 72 hours, if possible, except cases where the violation may not create a significant risk to the rights and legitimate interests of individuals.

The controller is also obliged to notify the supervisory authority, if the violation may pose a significant risk to the rights and legitimate interests of data subjects, except cases when:

- The controller has taken appropriate technical and organizational security measures that make the data incomprehensible to any person except admitted ones. It can be, for example, encryption of the data;
- After the violation of personal data, the controller takes actions to ensure that the high risk to the rights and freedoms of data subjects is unlikely to materialize;
- When notification of each data subject will be accompanied by "disproportionate effort", in this case alternative communication methods may be used. (European Parliament, The Council of the European Union, 2016)

Failure to comply with these requirements entails liability in the form of an administrative fine of up to 10 million euros or in respect of organizations up to 2% of the global annual revenue of the previous fiscal year, whichever is greater.

3.3.16 Rights of personal data subjects

3.3.16.1 The right to access

GDPR establishes a more detailed right to access compared to Directive 95/46 / EC. Users have the right to request a copy of their personal data which is going to be processed, as well as information about the purposes of processing, the storing period, recipients of data, the logic of automatic data processing and the consequences of any profiling. Controllers

need to set up access request procedures and establish a mechanism which can verify the identity of the requestor. In cases where the controller processes "a large amount of information" about the data subject, he is entitled to require indicating specific data or processing activities. (European Parliament, The Council of the European Union, 2016)

3.3.16.2 The right to rectification

The data subject has the right to request from the controller the correction of inaccurate personal data concerning him or her. Taking into account the processing objectives, the data subject has the right to supplement incomplete personal data, submitting an additional statement. (European Parliament, The Council of the European Union, 2016)

3.3.16.3 The right to object

“The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her”:

- To complete a task performed in the public interest or in the exercise of controller’s official powers;
- For the purposes of the legitimate interests of the controller or a third party, unless fundamental rights and freedoms of the data subject prevail over such interests or require the protection of personal data.
- In this case the controller is obliged to stop processing of personal data unless the controller provides a convincing legal basis for processing that prevails over interests, rights and freedoms of the data subject. (European Parliament, The Council of the European Union, 2016)

3.3.16.4 The right to erasure

Unlike Directive 95/46 / EC, GDPR explicitly recognizes the right to erasure which is an expanded version of the so-called “right to be forgotten” recognized by the European Court in a case of Google Spain v AEPD and Mario Costea Gonzalez 2014 (European Court of Justice, 2014). The court demanded that search engines should remove links to web pages that appear when searching for the name of the requestor, unless the “prevailing public interest” does not justify the refusal of the search engine to satisfy the request.

Controllers should delete personal data without undue delay if one of the following reasons exists:

- Personal data is no longer needed for the purposes for which they were collected or processed;
- The data subject has withdrawn the consent on which the processing was based, and there is no other legal basis for processing;
- The data subject objects to the processing, and there is no legal basis for processing, or the data subject objects to the processing of personal data for direct marketing purposes;
- Personal data was illegally processed;
- In order to fulfill the obligations provided by the legislation of the EU or the respective Member State;
- If personal data were collected in connection with the offer of information society services directly to the child (European Parliament, The Council of the European Union, 2016).

3.3.16.5 The right to restrict processing

The data subject has the right to require "processing restrictions" for:

- The time required to verify the accuracy of the information if he assesses its accuracy;
- In cases when the controller no longer needs data, but the data subject needs them for a lawsuit when the data subject objects to the processing, but the controller seeks to prove that he has a legal basis for overcoming the objection;
- If the data subject requests a processing restriction, the controller must temporarily remove the data from the general registration system or from the public website to avoid further processing. (European Parliament, The Council of the European Union, 2016)

3.3.16.6 The right to data portability

In cases when personal data is processed using “automated tools”, GDPR grants special rights to data subjects:

- To receive personal data in a “structured, commonly used, machine-readable and compatible format”;
- To transfer such data to another controller;
- To require transfer of the personal data directly from one controller to another, if such transfer is “technically feasible”. (European Parliament, The Council of the European Union, 2016)

In relation to the controllers, GDPR establish responsibilities regarding the provision and transmission of data in the appropriate format. However, the preamble to GDPR states that it does not impose a duty on controllers to implement technically compatible technological systems for these purposes.

3.3.16.7 The right to be informed

The data controller is obliged to inform the data subject immediately after receiving data on all manipulations that will be carried out with the data, as well as indicate the basis for processing, period of storage, intention to transfer personal data to third countries, legitimate interest pursued, rights of data subjects and contact details of the Data Protection Officer. (European Parliament, The Council of the European Union, 2016)

3.3.17 Monitoring compliance with GDPR. Remedies

Each Member State shall appoint one or more independent public bodies responsible for monitoring compliance with GDPR in order to protect fundamental rights and freedoms of individuals and to facilitate the free circulation of personal data within the EU ("Supervisory Authority").

The Supervisory Authority of the state where the controller and processor are established is authorized to act as the lead supervisor for the transboundary processing activities conducted by the controller or processor.

Supervisory Authority has the following powers:

- To conduct investigations in the form of data protection checks;
- To gain access to any premises, equipment and data processing facilities of the controller and processor, in accordance with the procedural legislation of the EU or a Member State;

- To issue warnings and reprimands to the controller or processor performing processing operations that may violate the provisions of GDPR;
- To give instructions to the controller or processor to bring the processing operations in accordance with the provisions of GDPR;
- To impose a temporary or final restriction, including a ban on the processing of personal data;
- To impose an administrative fine in addition to or instead of the above measures, depending on the circumstances of each individual case. (European Parliament, The Council of the European Union, 2016)

Personal data subjects whose data is not processed in accordance with GDPR are entitled to file complaints to the supervisory authorities. Such bodies are obliged to inform the data subjects about the progress and results of the complaints.

Data subjects and other interested persons have the right to go to court in connection with certain acts and decisions of supervisory authorities:

- Any person - in respect of legally binding decisions taken by the supervisory authority concerning his or her;
- Personal data subjects - if the supervisory authority does not consider the complaint or does not inform the data subject about the progress and results of the complaint within 3 months;
- Data subjects whose rights have been violated have the right to file a lawsuit against the controller or personal data processor responsible for the alleged violation;
- Any person which suffered damage as a result of a violation of GDPR is entitled to receive compensation from the controller or processor.

Responsibilities between controllers and processors are distributed as follows:

- Controllers are liable for damage caused by the processing of personal data that does not comply with GDPR;
- Processors are only liable for damage caused by any kind of processing which violates obligations imposed on the processors by GDPR, damage caused by external processing, processing which is in contrary to legitimate instructions of the controller.

Controllers and processors who participate in the same personal data processing are responsible for any damage in full. However, the processor or a controller, who is responsible for the payment of damages, has the right to seek compensation from other relevant parties corresponding to their part of damage (Information Commissioner's Office, 2017). At the same time, GDPR explicitly states that compensation can be recovered in respect of both monetary and non-monetary damages.

3.3.18 Administrative fines

Supervisory Authorities have the right to impose significant administrative fines on controllers and data processors, instead of or in addition to other violation penalties.
In a case of a minor breach or the penalty places a disproportionate burden on the individual, the supervisor may impose a reprimand, instead of a fine.
The regulation provides for two grades of fines depending on the types of violations.
Violation of the following provisions will entail administrative fines of up to 20 million euros or up to 4% of the global annual turnover, whichever is greater:

- Basic principles of processing, including conditions for consent (Articles 5, 6, 7 and 9 of GDPR);
- Rights of data subjects (Articles 12-22 of GDPR);
- Transboundary transfer (Articles 44-49 of GDPR);
- Obligations under the laws of member states, made in accordance with Chapter IX of GDPR;
- Failure to comply with the procedure established by the supervisory authorities.

The remaining violations will entail administrative fines of up to 10 million euros or, in the case of companies, up to 2% of annual global turnover, whichever is greater. In particular, the violation of the following obligations:

- Obtaining consent to the processing of data relating to children (Article 8);
- Introduction of technical and organizational measures to ensure the protection by design and default (Article 25);
- Obligations of joint controllers, coordination of their compliance with the requirements of GDPR (Article 26);
- Obligations of controllers and processors not established in the EU, appointment of representatives (Article 27);

- Obligations of controllers in connection with the involvement of processors (Article 28);
- Obligations of processors regarding attracting subcontractors only with the prior consent of the controller and data processing only on the basis of the instructions of the controller (Articles 28-29);
- Record keeping of personal data processing operations (Article 30);
- Obligations controllers and processors to cooperate with supervisory authorities (Article 31);
- Introduction of technical and organizational measures (Article 32);
- Obligations regarding violation reporting in the cases established by GDPR (Articles 33-34);
- Conducting an impact assessment on data protection (Articles 35-36);
- Appointment of DPO (Articles 37-39).

If GDPR does not establish administrative fines for any violations, EU Member States are obliged to create their system of fines and notify the Commission of any relevant legislative changes. (European Parliament, The Council of the European Union, 2016)

3.4 General Data Protection Regulation. Issues and difficulties

The GDPR, as a completely new phenomenon for the European Union, is controversial due to its new provisions and the rights/obligations granted to data subjects and controllers.
Like any law, it has both positive and negative sides, considering that GDPR is a completely unprecedented legislation for the whole world. It is difficult to overestimate its impact on European business and on ordinary users, it captures a huge part of the lives of EU and non-EU citizens.
Despite the fact that GDPR was developed primarily as a response to uncontrolled processing of personal data by global digital and advertising platforms, it ultimately affects almost any business that works with individuals in the EU (regardless of their citizenship and residence).
Therefore, it is rational to consider the key problematic issues in the sphere of its influence on business and individuals.

3.4.1 General Data Protection Regulation and Business

3.4.1.1 Bureaucratization

One of the problems that primarily concerns business is bureaucratization.
In the case of GDPR, the European Commission is willing to control as many areas as possible in order to protect citizens and anticipate future changes. However, this is not always justified, an excessive desire for regulation hangs heavily on business as well.
Business has to forever be torn between the need to provide a service quickly and conveniently and the creation of barriers to intruders. No one will order pizza through the app if it requires proof of identity by visiting the office or using ingenious information protection tools. Thus, bureaucracy, which requires constant consent requests for data processing, is very burdensome for customers. This, in turn, leads to the fact that customers are turning away from companies. Now, in the era of mobile technologies, the usability of online services and applications is very much appreciated, moreover, it is almost the main factor in attracting new customers and preserving existing ones. The organization itself sees food delivery as its main task, not the safety of customer information. Of course, with time, when compliance with GDPR becomes ubiquitous and people become accustomed to this format of relations, the need to give their consent to data processing will not cause such a reaction. But now, it frankly interferes with business (Tolstov, 2018).

3.4.1.2 Fines

A lot of talk and criticism goes to GDPR associated with the values of fines. The companies that are best prepared for GDPR are large: Facebook, Google, Amazon — those who have the money to join their technical and legal teams for maximum compliance. However, small and medium businesses may be less prepared, which makes them more vulnerable to possible fines and penalties.
The maximum fine for violation of GDPR norms is up to 20 million EUR, or 4% of the violator’s turnover (the largest amount is chosen). Such punishment is imposed for serious violations, for example, the processing of personal data without the consent of customers, discrediting confidential information or violation of product design rules.
GDPR provides a flexible multi-level approach to fines. In particular, the company may be fined 2% for not notifying the supervisor and data breach subject or failing to assess

potential damage. Of course, a small business just physically cannot pull out this kind of burden without going broke. There are initiatives, mostly from businesses, to reduce potential fines. The main argument for this is that if a hacker broke into a company system and requires a ransom, in most cases the ransom will cost companies less than paying a GDRP fine (Stolton, 2018). However, it should be noted that initially the penalty rate was much higher, and only after long discussions it was reduced to the existing level.

Even though the fines are high, this does not mean that the company will be charged mentioned amounts by default. The decision on penalties and fines depends on a huge number of factors. This may be the general level of compliance with GDPR, or the general level of data protection against breaches, or what actions were taken in the direction of GDPR, or how privacy by design is respected, or the existence of legal grounds for data processing and thousands of other factors.

The fact is that according to the law, each case of violation of the GDPR is considered individually in the context of all the above factors. And fines, in turn, must be „effective, proportionate and dissuasive" (European Parliament, The Council of the European Union, 2016). GDPR considers nature, gravity and duration of the infringement taking into account the nature, scope and purpose of the processing concerned, as well as the number of data subjects affected, and the level of damage suffered by them (European Parliament, The Council of the European Union, 2016).

Austria released its first GDPR fine for an organization that installed a surveillance camera before the entrance, and recorded images the sidewalk. Supervisory Authority issued a moderate fine, 4,800 euros, which is much less than maximally possible fine (Privacy Laws & Business, 2018). The mechanism of GDPR fines is shown in the Figure 1:

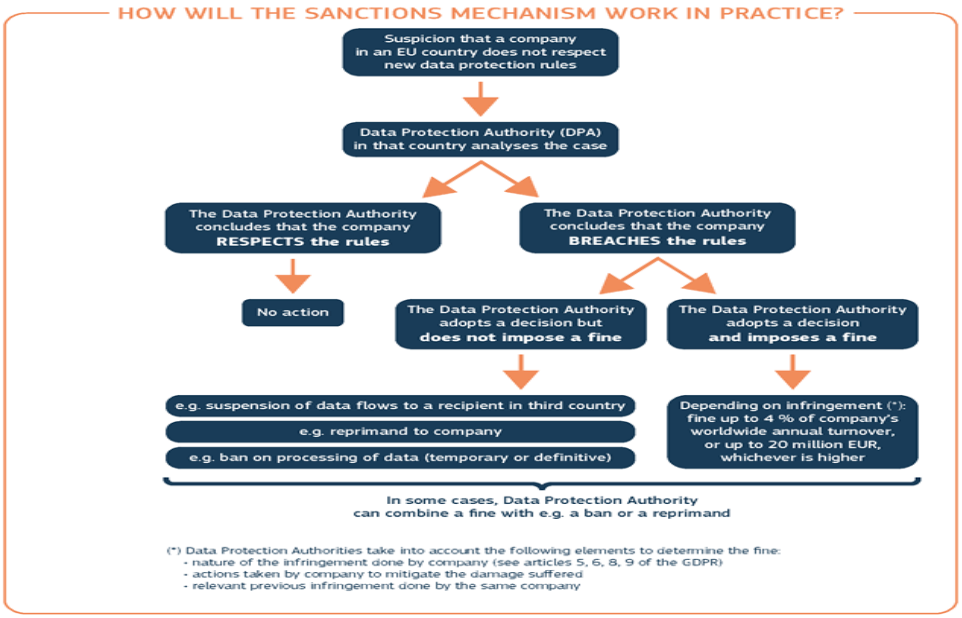

Figure 1 - How will the sanctions mechanism work in practice

Source: European Commission (2018)

Thus, it is obvious that the imposition of fines depends not only on the level of violations, but also on individual indicators. Both monetary and non-monetary penalties can be applied.

Interestingly, if a complaint was filed against a violation of GDPR, which concerns data processing, but most likely will not damage the rights and freedoms of data subjects, the Supervisory Authority must first look for a way to make an amicable settlement with the controller, and only after that failure apply its powers. (Lyons, 2016)

3.4.1.3 Costs of compliance

The 500 largest corporations in the world was going to spend a total of 7.8 billion USD to match GDPR (Jeremy Kahn, 2018). The Czech Republic spent about 25 billion crowns for GDPR compliance. According to Czech Chamber of Commerce, majority of Czech companies pay around 50000 CZK for GDPR compliance, and more than a fifth of large companies with more than 250 employees has spent over half a million crowns on these measures. (Globe24.cz / ČTK, 2018)

It is impossible to indicate the cost of GDPR compliance for each business, since there are a lot factors that affect the costs: type and volume of personal data processed, size of organization, number of employees, type of business etc.

A research conducted by the Ponemon Institute, based on data from 53 companies, showed a linear dependence of the size of the company and the number of employees on the expenses for compliance with the GDPR, which is illustrated in the Figure 2:

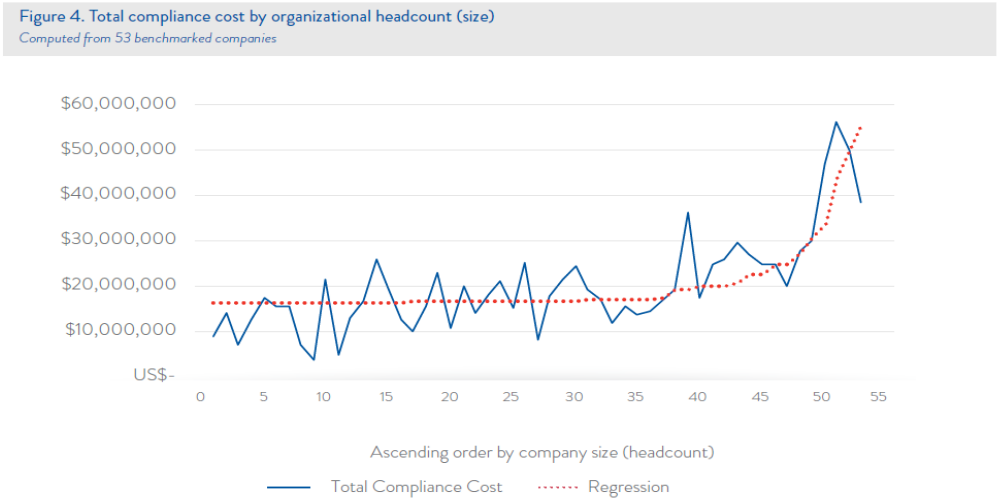

Figure 2 - Total compliance cost by organizational headcount (size)

Source: Ponemon Institute LLC (2017)

British researchers came to similar results and went even further by analyzing the average GDPR costs per employee. The average cost of introducing a GDPR per employee is kept at a stable-average level with little variation, which is illustrated on the Figure 3:

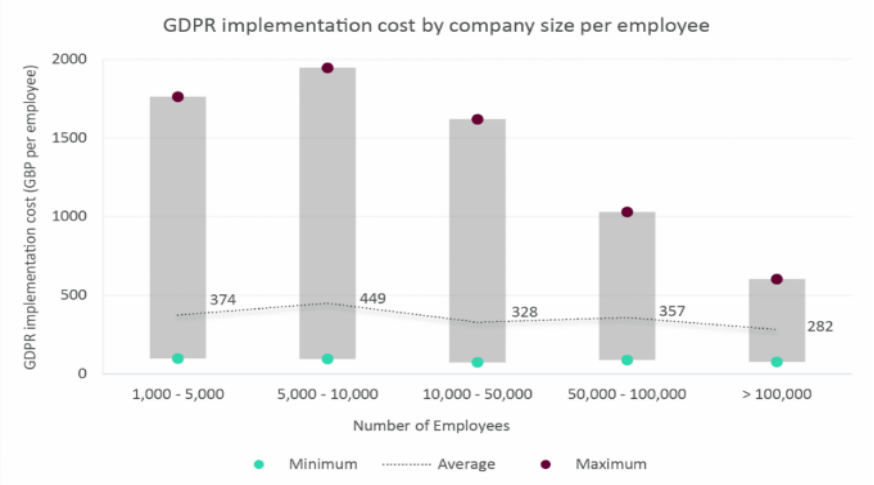

Figure 3 - GDPR implementation cost by company size per employee

Source: Sia Partners (2018)

Nevertheless, the size of the company is not the only factor that influences the cost of introduction of GDPR. For example, a construction company that employs several dozen people from different professions may have significantly lower costs for GDPR

compliance than a company with five employees, which, for example, is engaged in reviewing customers preferences in social networks (Januš, 2018). Because the type and amount of work with personal data is completely different.

Therefore, the calculation of expenses for compliance is strictly individual for each company. However, we can highlight the main compliance-related expenses:

- Data protection and enforcement activities;
- Incident response plans;
- Compliance audits and assessments;
- Policy development;
- Communications & training Staff certification. (Ponemon Institute LLC, 2017)

Even though spending on GDPR strongly hit on any business, the cost of non-compliance is estimated much higher. In the modern world, non-compliance threatens not only monetary penalties but also reputational or customer losses, which potentially will lead to much greater financial consequences. Therefore, there is only one conclusion: it is worthwhile to keep abreast of the times and not to save on GDPR. (Wright, 2018)

3.4.2 General Data Protection Regulation is Social Media Marketing

A modern web page works not only with content, but also with visitor data. This data provide communication with social networks, give access to analytics, schedules, the possibility of conducting electronic mailing and so on and so forth. Without this data, the success of online marketing would be zero. The reason that GDPR has now become burdensome for marketing is the fact that previously all these data were practically unprotected (the protection was weak). Many laws on protection were created a quarter of a century ago, and with the development of digital technology, it is simply morally obsolete. And the new GDPR introduces privacy laws. Compliance with GDPR for online marketing leads to several problems, which boil down to even more bureaucratization.

The previous legislation implied the concept of implicit consent, which allowed the use of marketing activities to data subjects, without their direct permission. According to GDPR 'implied consent' or 'soft opt-in' are no longer an option for Business-to-Customer data (Askari, 2018). GDPR commits the business to ask for explicit “opt-in” to interact with the personal data, and in some cases, even “double opt-in” may be required.

Let’s consider the impact of GDPR on the example of a small commercial site which is primarily used for marketing purposes.

Most likely, any modern website uses Google Analytics to collect user IDs, cached personal data, IP addresses, cookies, or behavioral data. To comply with GDPR site needs to make the data anonymous before saving and processing or place a banner on the site that would inform about the use of cookies and request permission from users before entering the site.

If the site is using advertising in the format of retargeting, incl. Facebook pixel, it needs to notify users when they visit the site and get their explicit consent. If site publishes sponsored content, it needs to ask the advertiser if he uses tracking pixels, cookies, and why. If the company collects personal information for remarketing using pixel and cookies, this will also require user consent when entering the site.

Email newsletters subscription is commonly used in online marketing. However, ticking items should be present in the registration form, putting user agrees with everything that user is subscribed to. If tracking pixels are embedded in the newsletter (to find out when letters are opened), the user should know about this before subscribing – site should post a noticeable message about this.

If a site places ads of a third-party advertising server, it will also need to obtain the consent of the users before entering the site. Only in this way a third-party server will be able to use user data for advertising and marketing.

If a site places affiliate links, it will need a consent to the use of cookies for each individual post. Consent is required before the visitor clicks the affiliate link, because the cookie is placed in the browser to track activity.

Before a user can leave a comment or feedback, it is also necessary to get a consent (ticks) and inform that a site will save comments and, if necessary, information related to the content, data and computer IP addresses.

These items are not significant for the marketing activities from the point of view of the user. However, this complicates the work of marketers, limiting the amount of information received, narrowing the range of work with information. The constant demand for consent to any Social Media Marketing activity demotivates users and complicates the site’s interface.

3.4.3 General Data Protection Regulation in Blockchain and Cloud technologies

The blockchain technology was introduced in public use relatively recently, but confidently occupied its niche in the field of IT technologies. The use of technology is quite wide: from financial services to energy and video games. Initially, the GDPR was created to affect centralized systems, where data subjects interact with data processors. Similar interactions are easy to track and control. This applies to social networks or cloud storage.

However, the principle of the blockchain technology is decentralized and radically different from others. It can be presented as an account book, which has each participant of the event and which is constantly updated. In fact, any event can be written in this book - from financial transactions with cryptocurrencies Bitcoin, Etherum, etc., to the results of voting in the presidential election or identification data (Bazanov, 2017). The blockchain chip is that the pages (read the blocks) of this book are simultaneously stored with all users of the network, are constantly updated and refer to the old pages (for more details, see the bitcoin mining article). And if someone tries to deceive the system by tearing out or pasting a page into a book, the system will immediately turn to tens of thousands of other versions of this book and find a discrepancy in the block structure. Thus, it is almost impossible to change the data in the blockchain.

This goes against GDPR (Article 17), which guarantees the right to be forgotten, and any user can request to delete data from blockchain chains. And it causes problems. There is a principle of immutability of entries that does not allow changing of any data contained in the blockchain. We cannot remove one fragment from an already created chain without affecting the entire chain. This means that once a chain has been created, it must remain unchanged throughout its existence. Because of the design features of the blocks, all the information that is contained is completely public, but is very well protected from unauthorized access, which soothes the situation, but does not solve it. One of the ways to solve this problem is to use pseudoanonymization of data inside the blockchain and store sensitive personal data outside the network in other protected places (Lima, 2018).

Among other things, GDPR applies to Cloud technologies - data processing technologies that provide the user with computer resources as an Internet service. The user has access to his data, but cannot manage the infrastructure, the operating system and the software itself, with which it works.

According to GDPR, user data can only be stored for a certain time and should be corrected or deleted on the first request. Cloud storage can be physically located in different places, or even countries, with different legislation and under different jurisdictions. Thus, it makes data management difficult when it comes to different jurisdictions. Moreover, data deletion is also problematic, given the availability of backup copies of data from different cloud service providers. In addition, data may be stored outside the European Union. Controllers need to develop a special strategy for several countries to meet the adequacy requirements and data localization laws (Tolsma, 2018).

3.4.4 General Data Protection Regulation and ordinary citizens

Despite the fact that GDPR is designed to protect the personal data of EU citizens, it also has problematic consequences that citizens face:

- **Restricting user access to certain information resources**

  When GDPR came into force, one of the immediate results was an increase in the number of websites that restricted access to European users. In particular, this applies to the United States.

  It was announced that some major American media publishers, such as the Chicago Tribune or the Los Angeles Times, had partially blocked their sites for many European users.

  Of course, companies had 2 years to prepare, but many of the companies were not prepared or did not consider preparation as an option. Too much, apparently, was the fear of being sanctioned for possible breaches of confidentiality (Forbes Technology Council, 2018).

- **Restrictions on access to Android and Apple software**

  Most applications in the Apple and Android app stores collect some personal information, and most of these developers are too small to manage this data and be responsible for its proper use. This means that they also restrict access to these applications for European users.

- **Photographs and video filming**

  Photographs, video filming are also part of GDPR, this does not affect ordinary citizens. Difficulties may arise from photographers and bloggers. After all, they shoot the streets, show the faces of people, and at the same time the activity is a

commercial one. Thus, it imposes a number of difficulties on the implementation of the activity. (Tolstov, 2018)

- **Potential increase in the number of paid services**

  We all use smartphones and social networks. And if the service is free, it means that the product is data. We constantly use Facebook, Twitter, YouTube and other networks, not understanding how such a business works. If GDPR begins to stifle business with regulations and rules, there will be no other option than the paid model. A typical example of this is YouTube, which has already introduced paid subscriptions and monetizes content in every possible way (Singleton, 2016).

- **Poor customer service.**

  Too many restrictions, regulations and bans lead to poor customer service. This is especially true of services such as hotels, where customer interaction is brought to the fore. An abundance of consents and bureaucracy will inevitably degrade the quality of the service. (Forbes Technology Council, 2018)

4 Practical Part

In the practical part, a brief description of the company will be given, its economic indicators and structural organization will be considered. An analysis of the current state of affairs in the field of personal data processing will be conducted, and GDPR implementation project will be developed and applied. In addition, an assessment of the risks of the introduction of this project will be made, the costs and consequences of its application will be assessed. It was decided to choose a large enough hotel as a basis for analysis, since the hotel activity is closely related to the interaction with personal data, and the introduction of the GDPR could potentially affect the conduct of its business activities.

4.1 Characteristics and key performance indicators of the chosen company

The following chapter deals with the analyzed company. It is described how the company developed over the years, basic information on the organizational structure and number of employees, a breakdown of the services and products offered. Finally, an analysis of costs, yields and economic results is carried out.

4.1.1 Company description and its history

Analyzed company Tolleson s.r.o was founded in 2005 as a joint-stock company, with a mounting capital of 200000 CZK. The main activities of the company were:

- Mediation in business and services;
- Wholesale and retail trade;
- Real estate, property management and maintenance.

In 2007, the company was bought by a new owner and reorganized into limited liability company (Tolleson s.r.o). Until 2014, the company did not generate revenue, working with zero profit. The new owner of this company owns 3 hotels in Italy and Croatia and specializes in the hotel industry. It was decided to build a hotel in Prague, as in the most attractive tourist destination in central Europe. The construction of the hotel was started in 2014 and the “Hotel Royal Prague” brand was registered. Thus, the focus of the company’s activities was shifted to a completely new sector: “rental properties, apartments and non-residential premises”. Construction was completed in 2016, and the company started to

provide hotel accommodation services. The hotel is accredited with 4 stars and provides an exceptional service to guests and customers.

4.1.2 Basic information

This chapter is intended to describe organizational structure, staff development and key indicators of economic activity

4.1.2.1 Organizational structure

Since the company has completely changed its vector of activity, it makes sense to consider its structure and economic activity from the moment of establishment of the hotel, since previous periods are irrelevant for this study.

The organizational structure of the hotel is typical for all the hospitality enterprises. It includes all the key figures responsible for the implementation of hotel activities. The following Figure 4 describes an organizational structure of the hotel:

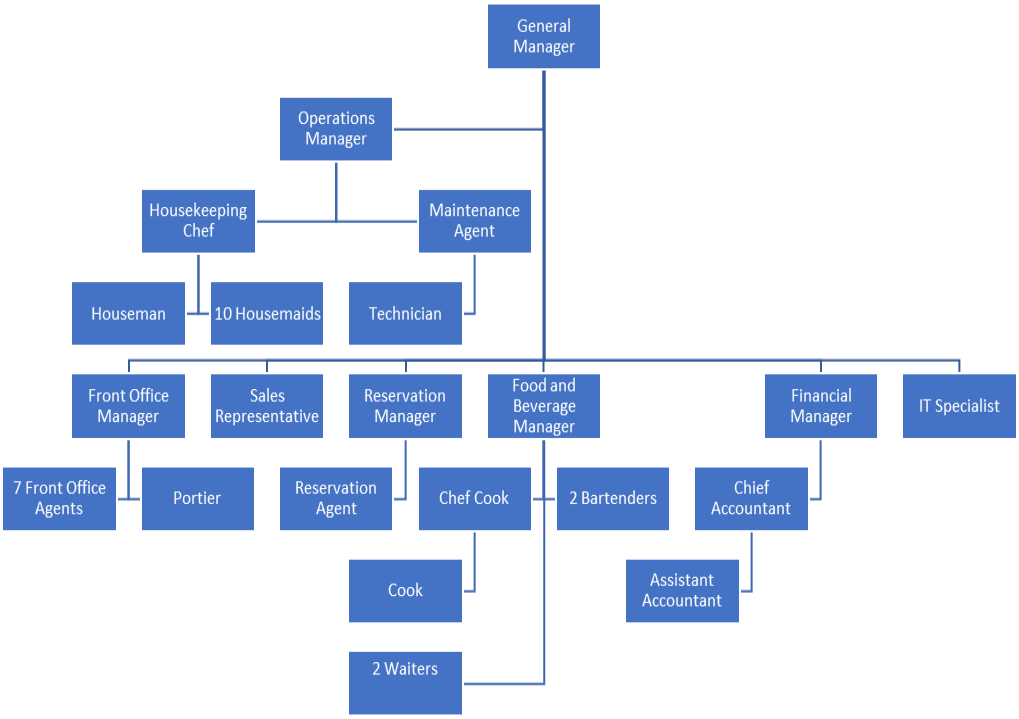

Figure 4 - Organizational structure of the Hotel Royal Prague

Source: own work (2019)

4.1.2.2 Employees and staff development

This structure includes both permanent employees of the hotel and outsourcing employees who are hired to fulfill certain hotel needs. Usually, the outsourcing workers are all technical staff and cleaners. The staff development is described in the Figure 5:

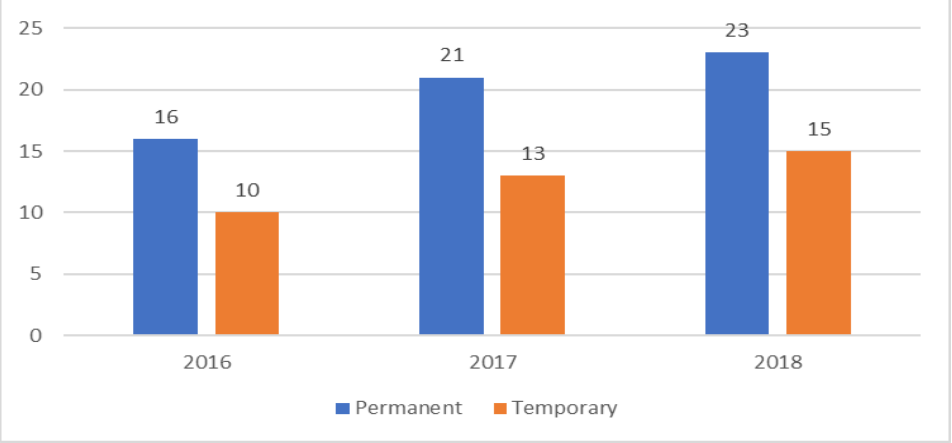

Figure 5 - Staff development

Source: own work (2019)

As it is seen from the graph, the number of employees is increasing from year to year, which indicates the development of the hotel since its opening. In 2017, new reception staff were hired in addition to the existing because the demand for hotel services increased. In addition, a sales agent was hired to establish relationships with corporate clients and to organize pricing policies. Since 2018, the restaurant at the Hotel "Oro Nero" began to work, which required to hire new employees, and the growing popularity of the hotel required additional temporary staff. These factors and led to an increase in the number of hotel employees.

4.1.2.3 Analysis of costs, revenues and profit after tax

This part of the thesis compares the costs produced with the company's earnings and the accounting of the post-tax financial performance during 2016-2018.

The Table 1 deals with the costs, revenue, and profit after tax in the 2016-2018:

In EUR	2016	2017	2018
Revenue	4222548	4398811	4520351
Costs	886735	923750	1356105
Profit after tax	253528	2639286	2260175

Table 1 - Costs, revenue and profit after tax (2016-2018)

Source: adapted from hotel financial statements (2016-2018)

The Figure 6, which was created on the basis of the table gives a better overview of the development of the key economic indicators in 2016-2018:

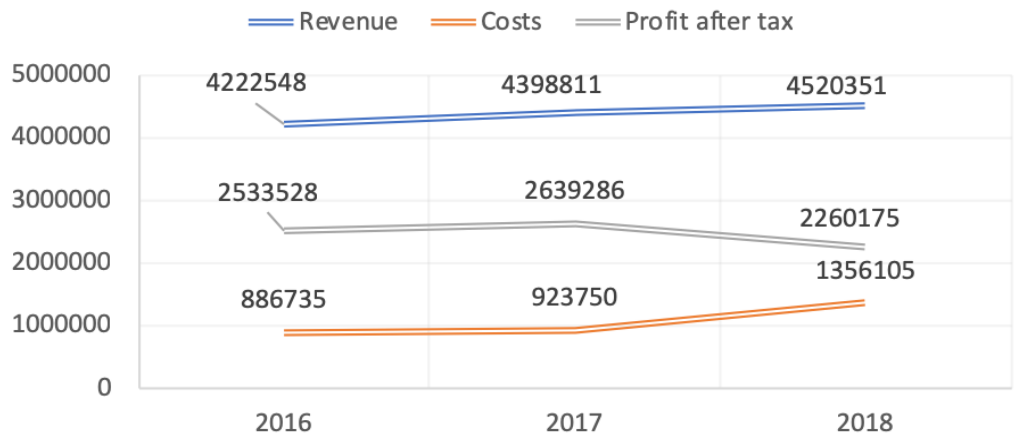

Figure 6 - Costs, revenue and profit after tax in the 2016 - 2018

Source: adapted from adapted from hotel financial statements (2016-2018)

From the graph it is evident that the company was getting more and more costs in 2016-2018.

A simultaneous jump in costs and revenues in 2018 can be observed. This is a result of the opening of the restaurant at the hotel, as it required additional costs for equipment and supplies, but provided an additional source of revenue for the hotel.

Due to the fact that the company hired additional employees in 2018, there was an increase in administrative costs, namely staff costs, which rose more than four times over 2016. Although the company recorded revenues higher than in 2017, the enormous increase in costs also affected the loss of profit and loss of the company.

4.1.2.4 Portfolio of services

The purpose of this subchapter is to describe what services the given company provides.

The hotel has 200 rooms and provides the following services:

Standard services:

- 4 * class living conditions;
- provision of various information;
- cleaning of premises;
- sauna, swimming pool, fitness room;

- parking lot.
- wireless Internet;
- free breakfast.

4.2 Analysis of the current state of personal data processing

This chapter is intended to analyze the current state of affairs in the field of personal data processing.

4.2.1 Analysis of internal regulations

The company has no internal documents in the field of collection, protection and processing of personal data of both employees and hotel guests.

4.2.2 Analysis of the current security of personal data

For the processing of personal data, the company uses internal software which was solely developed for this company. The hotel has an internal local network through which data is accessed. Regardless of the fact that the hotel software requires Internet access to work, access to the stored data can be obtained using only the local network.

The company keeps the data in both electronic and printed form and is thus accessible to employees. Electronic data is located on the protected shared drive and can be accessed only by certain hotel staff. Each user must be authorized to access. Access passwords are a security feature, as they have to meet security requirements. Each of the passwords must consist of several characters, they must contain both upper- and lower-case letters and numbers.

Key hardware devices such as servers, routers, back-up resources, etc. are located at separate locked data center room in order to prevent access to unauthorized persons and maintain stable operating conditions.

A backup copy of all the data stored on the main hard disk is created daily. It is automatically recorded on a spare hard drive. It is done in order to prevent the loss or damage of important data. In the case of the primary hard disk failure, the data will be recovered from the spare hard drive.

The company uses Kaspersky antivirus to protect against viruses and potential data hacking. Regular and automatic updates are provided by the software manufacturer.

Paper data is stored in the archive, in which it falls upon the expiration of the work shift. During the working shift data is stored in non-closing drawers. However, every hotel employee has access to these files, therefore such data protection is unacceptable.

4.2.3 Personal Data Analysis

Completing of the analysis will give us the necessary insight of the scope of personal data as well as the legality of its processing with respect to legal basis and possible storage period. The analysis is also essential for the distinction between personal data and special categories of personal data (sensitive personal data) that require a higher level of protection and need a written consent. They can only be processed under more stringent conditions and, in particular, concern health or biometric data. It is also necessary for the implementation of the GAP analysis to understand the direction and need for improvement. To carry out data analysis it is necessary to take into account several factors:

- Types of data /documents containing personal data.
  The hotel has to collect only those data that are necessary for the implementation of hotel activities and ensure the comfort and safety of the guest.
- Categories of personal data.
  In the context of hotel activities, the hotel collects identification data, contractual data, contact information, payment information, safety data, and additional data.
- Is the data collected is sensitive?
  The hotel collects both sensitive personal data and ordinary ones.
- Lawful basis for processing
  As already indicated, the GDPR provides for several grounds for processing. In the case of a hotel, the grounds can be: performance of the contract, legitimate interest, fulfilling the statutory duty, written consent.
- Possible period of storage of personal data
  Personal data must be stored for the period prescribed by law, and no more than is necessary to fulfill the conditions of the contract and the internal provisions of the hotel (in case of legitimate interest).
- Purpose of processing.
  The purposes may be very different from fulfilling obligations under the law to protecting property and hotel guests

The results of the analysis are grouped into 2 different tables: Analysis of personal data of hotel guests (Appendix 1) and Analysis of personal data of employees (Appendix 2).

4.2.4 GAP Analysis

Based on the analysis of the current state of processing of personal data and taking into account the fact that the hotel is almost completely not ready for the GDPR, it will be necessary to carry out the whole GDPR implementation procedure:

- Ensure the required security measures in the field of IT and paper data storage;
- Create Records of Processing Activities;
- Conduct Data Privacy Impact Assessment;
- Update hotel website;
- Assign Personal Data Protection Officer (DPO);
- Conclude agreements on the processing of personal data by employees (processors);
- Develop a consent template;
- Develop a data leakage reporting procedures and templates;
- Develop a sample answers to data subject requests;
- Introduce internal regulations:
  - Privacy Policy;
  - Personal Data Protection Directive;
  - Directive on the protection of the personal data of employees;
  - Directive on the processing of sensitive data and personal data of children;
  - Supervision and Privacy Guidelines;
  - Data Protection Officer Policy;
  - CCTV Policy;
  - Revocation and Restriction Guidelines;
  - Policy on the rights of data subjects;
- Establish control mechanism;
- Conduct employee training.

Given the fact that the author does not have in-depth legal knowledge, it was decided to seek legal advice from Goodking Advisory s.r.o, whose staff kindly agreed to help in writing this thesis work providing document templates and consultations.

4.3 GDPR implementation project

One of the goals of this thesis work is to develop the case study on the GDPR implementation in the given company. The project section will remove the discrepancies found in the GAP analysis of the current state of processing of personal data to make the hotel GDPR compliant.

4.3.1 Project activities and timetable

On the basis of familiarization with the requirements of the GDPR described in the theoretical part of the thesis and analysis of the current state of data processing and GAP analysis the timetable for the upcoming activities was completed. The input analysis was performed within 30 business days. Its implementation began in September 2018. The time schedule of the project is processed using the CPM - Critical Path Method, which is one of the basic deterministic methods of network analysis. The goal is to determine the duration of the project based on the length of the so-called critical path. First of all, the individual project activities that determine the duration (in this case, the duration is determined in days) are determined, and the previous activities are determined - for each activity, it must be clearly stated which of the activities must be preceded.

The actual activities for the timetable for the implementation of the General Data Protection Regulation are shown in the Table 2:

Activity	Description
1	Ensure the required security measures in the field of IT and paper data storage
2	Update hotel website
3	Create Records of Processing Activities
4	Conclude agreements on the processing of personal data by employees (processors)
5	Assign Personal Data Protection Officer (DPO)
6	Conduct Privacy impact assessment (DPIA)
7	Develop a data leakage reporting procedures and templates
8	Develop a sample answers to data subject requests
9	Develop a consent template
10	Establish control mechanism
11	Conduct Employee training
12	Introduce internal regulations

Table 2 - Activities for the schedule for the implementation of the General Data Protection RegulationSource: own work (2019)

The input data was processed in Excel in order to determine the shortest possible time for the project to be executed. Using a Beta distribution, where O is the minimum, P is the maximum, and M is the most likely duration, the formula for calculating the mean or expected time was:

Duration = (O+4M+P)/6

Using a Triangular distribution, the mean of the distribution is:

Duration = (O+M+P)/3

According to the calculations, the approximate time of GDPR implementation project is 22 days.

The tasks that are marked as critical cannot be delayed without delaying the project, they are: Introduce internal regulations, conclude agreements on the processing of personal data by employees (processors), establish control mechanism, conduct employee training.

The input data and the schedule together with a Gantt chart are grouped in the Table 3 and Figure 7:

GDPR IMPLEMENTATION SCHEDULE — **Critical Path Analysis**

Start Date	Finish Date	Days to Completion	No successor defined yet	Critical tasks
01.12.2018	03.01.2019	22,00		

Times (in Days)

Time Distribution: Triangular

ID	Task Name	Predecessors (Enter one ID per cell)										O (min)	M (most	P (max)	Duration (exp. time)	ES	EF	LS	LF	Slack
10	Start														0,00	*0,00*	0,00	0,00	0,00	0,00
110	Ensure the required security measures in the field of IT and paper data storage.											3	4	6	4,33	0,00	4,33	8,00	12,33	8,00
120	Update hotel website	220										3	5	9	5,67	12,33	18,00	14,33	20,00	2,00
130	Create Records of Processing Activities											1	1	1	1,00	0,00	1,00	15,00	16,00	15,00
140	Conclude agreements on the processing of	220	110									4	6	10	6,67	12,33	19,00	12,33	19,00	0,00
150	Assign Personal Data Protection Officer (DF	220										2	3	5	3,33	12,33	15,67	16,67	20,00	4,33
160	Conduct Privacy impact assessment (DPIA	130										1	1	1	1,00	1,00	2,00	16,00	17,00	15,00
170	Develop a data leakage reporting procedures	190	160									1	1	1	1,00	4,00	5,00	19,00	20,00	15,00
180	Develop a sample answers to data subject r	160										1	1	1	1,00	2,00	3,00	17,00	18,00	15,00
190	Develop a consent template	180										1	1	1	1,00	3,00	4,00	18,00	19,00	15,00
200	Establish control mechanism	140										1	1	1	1,00	19,00	20,00	19,00	20,00	0,00
210	Conduct Employee training	220	200	190	180	170	160	##	140	130	120	1	2	3	2,00	20,00	22,00	20,00	22,00	0,00
220	Introduce internal regulations											10	12	15	12,33	0,00	12,33	0,00	12,33	0,00
1000	**Finish**	210													0,00	22,00	22,00	22,00	*22,00*	0,00

Table 3 - Global Data Protection Regulation implementation project schedule

Source: own work (2019)

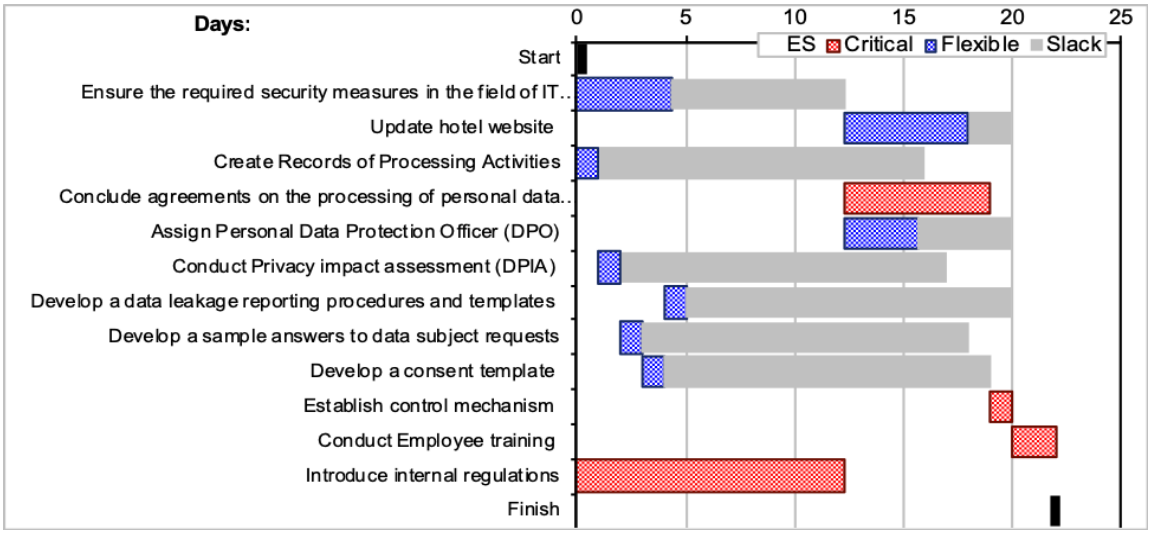

Figure 7 - Gantt chart for the General Data Protection Regulation implementation project

Source: own work (2019)

4.3.2 Ensure the required safety measures in the field of IT and paper data storage

4.3.2.1 Storage of electronic data

The Regulation does not directly regulate a specific type of security or encryption for certain processing activities or certain dates. Instead, it instructs controllers and processors to consider the sensitivity of the data processed and the impact on data subjects in the event of data leakage. In practical terms, if data from the hotel reservation system is leaked and freely available on the Internet, it may have a serious impact on data subjects in different situations. This booking system, like other systems or storage, must ensure that data will not leak. This is ensured by the fact that it is an internal software that is developed only for this hotel, and third parties do not have access to the data and the data is stored in the internal storage with a limited access. However, to ensure complete preservation, it was decided to add anonymization feature to the software to make sure that the data, even in the event of a leak, will not be processed and misused.

4.3.2.2 Flash Drives

Data storage for flash drives or external drives is the same as for any other storage. With the advent of GDPR, it is not possible to leave an unsecured flash containing unattended personal data.

It was decided to use software encryption of data SanDisk Cruzer Force. It is a software that decrypts files on the computer in which a flash drive is inserted. If the computer does not have this software installed, it is not possible to work with the files. The advantage of this solution is significantly low price compare to hardware encryption. The hotel bought 30 items of flash drives with the mentioned encryption.

4.3.2.3 Physical documents

The principles described in GDPR do not apply only to electronically stored data. They are also fully applicable to documents in paper form. The most common documents that contain personal information include contracts, invoices, orders, hotel registration cards etc.

As with electronic documents, the risk to data subjects in case of data leakage should be considered. It was decided to hang an electronic magnetic lock on the archive door and restrict access to this data only to hotel staff who process such data. Each employee will have a special magnetic card that unlocks only those premises to which the employee has a working relationship. In addition, it was decided to purchase special magnetic boxes for storing personal data during a shift, which can also be opened only with an individual magnetic key.

4.3.2.4 Mobile phones

Some employees, mostly management, have corporate mobile phones that they use for work purposes. Mobile phones are even more sensitive because they are often linked to a working email, contacts, or corporate document store. Therefore, we expect a higher level of security for mobile phones as a necessity for most subjects. Employees are required to ensure the safety of data on the phone using:

- Access security. Employees are required to set up a password or retrieving a fingerprint before the phone can be used.
- Data storage security. Employees are required to encrypt mobile phone storage. All the employees have iOS-based phones, and encryption is already turned on automatically.

4.3.2.5 Camera systems

Data from camera recordings are considered to be personal data if, on the basis of these records, a particular person can be identified directly or indirectly (image or sound recordings very often allow indirect identification of the person). Identifying occurs primarily when it is possible to recognize the characteristics of a particular person, such as a face image, on the camera record. In conjunction with other data, the person can then be fully identified.

It is necessary to notify guests and any visitors that video surveillance is being conducted. For these purposes, we have specially developed an index plate which contains:

- A camera picture;
- Description of the image in the text ("the space is monitored by the camera system with the recording");
- Under this, the DPO name and a link to a hotel's Data Processing Policy are identified.

The image and description are clearly and legibly visible from a distance of 2-5 meters. According to the proposed format, the hotel ordered 50 index plates with abovementioned inscriptions to hang in the necessary places.

4.3.3 Create Records of Processing Activities

Under Article 30 of the GDPR, most controllers and processors are required to keep records of the processing activities for which they are responsible. Records of Processing Activities are a record of how hotel processes personal information, where it is stored, and where it was forwarded. This is a living document and if it was created, it is possible to update it when the process of processing personal data changes or some new processing begins.

Since our organization processes specific categories of data, such as sensitive data it is necessary to keep the Records of Processing Activities.

In terms of hotel activity, we have developed Records for two categories: employees and hotel guests. Considered processing activities are grouped in the Table 4.

Guests	
Reservation system	The record contains data obtained when sending a booking request.
Provision of accommodation services	The record contains information when providing accommodation services.
Evidence and transfer of accounting documents	The record contains work with invoices and other accounting documents.
Ensuring Safety	The record contains work with security system
Employees	
Employment	This activity describes all the agenda for the recruitment of a new employee
Attendance	This record describes employee attendance records.
Ensuring organization security	This record describes processing of personal data for employees to ensure security.
Organization actions	A description of processing in case of a company event, team building, or training.

Table 4 - Processing activities for the Records of Processing Activities

Source: own work (2019)

4.3.4 Conduct Data Processing Impact Assessment

If the processing of personal data involves a higher risk to the rights and freedoms of the entities due to the fulfillment of certain processing parameters, the organization must develop a so-called DPIA.

The DPIA contains a general description of the risk processing, its operations and the assessment of the above risks for data subjects. DPIA is an important tool for ensuring and evaluating risks arising from processing activities. DPIA also includes suggestions of intended procedures, measures, safeguards, or mechanisms to reduce this risk.

If there is no risk identified, it is necessary to document the reasons why the DPIA will not be implemented. There is no need to conduct an DPIA because hotel believes that the personal data is not at risk, since the processing operations performed by the controller do not pose the following risks:

- Evaluation of data subjects: not implemented
- Automated decision-making on data: not implemented

- Systematic monitoring: not performed
- Data processed on a large scale: not implemented
- Data file merge: not implemented
- Venerable data: not processed
- Use of innovative technologies: not implemented
- Obstruction in the exercise of rights: processing does not arise

That’s why the document which describes mentioned reasons was created.

4.3.5 Update hotel website

In accordance with the GDPR, the hotel must update its website. The hotel website is used primarily for direct booking of hotel rooms and services. Therefore, first of all, it is necessary to place a link to the hotel’s Privacy Policy so that the users have the opportunity to get acquainted with the main provisions. It is necessary to update hotel reservation forms in accordance with the GDPR. In addition, the hotel uses cookies, it is necessary to add a consent form for the use of cookies in this website.

Since the hotel does not use user data for marketing purposes, it simplifies filling out registration forms and does not require a separate consent. The data of users who were provided through the booking form are part of the contract, and thus do not require a direct consent for its usage.

4.3.6 Assign a Data Protection Officer

GDPR clearly provides for cases where the appointment of Data Protection Officer is necessary.

- The processing of personal data is carried out by a public authority or a public body.
- If the organization's core activity is activities that require the extensive processing of sensitive personal data or personal data relating to convictions in criminal matters and offenses.
- Where the main activity of an organization is in activities for which there is a need for extensive, regular and systematic monitoring of data subjects.

The Data Protection Officer will fulfill the role of the so-called Privacy Reviewer. Its main task will be to ensure compliance with the Regulation and be a contact person for both the personal data subjects (especially those) and the Supervisory Authority.

In the context of its activities, the hotel falls under the third category, since it possesses security cameras which systematically monitor public areas of the hotel and has a loyalty program for return guests. Thus, the appointment of the DPO is a necessity. There is a possibility of appointing one of the existing employees on a voluntary basis for the post of DPO, however, the employees do not have enough competence. It was decided to use the services of an external DPO.

4.3.7 Conclude agreements on the processing of personal data by employees (processors)

Within the framework of the GDPR, it is obligatory to conclude agreements on the processing of personal data by employees. This agreement governs the duties and rights of the controller and the processor, the categories and types of personal data processed, the type and extent of the processing, purposes and legal titles, this agreement is based on the following clauses:

- The processing of personal data based on documented data and valid controllers' instructions that determine the purpose and means of processing. It addresses the issue of the transfer of personal data to third countries and international organizations.
- The agreement ensure confidentiality for people involved in the processing.
- The controller ensures the security of the processed personal data based on sufficient organizational and technical measures.
- It is described in which cases the data security breach / leakage is the responsibility of the controller or processor
- If the processor wants to get involved in the processing of another processor, he/she can only do so on the basis of controller's authorization.
- Synergies in the behavior of the controller and the processor, such as the obligation of the processor to ensure synergy in the performance of the controller's duties, to respond to requests and complaints from data subjects (right of cancellation, right of portability, right of access).

- The processor is also required to allow audits and inspections to be carried out from the controller side.

Within the framework of this enterprise, data processing contracts were concluded with all persons related to data processing.

4.3.8 Develop a consent template

Based on the analysis of the personal data collected, it is clear that the hotel does not collect personal data that requires direct consent for processing, either in the case of employees or in the case of hotel guests. However, there may be situations when the guest himself wishes to provide personal data to the hotel to meet his/her own needs or to receive exceptional services etc. For situations that may happen it is necessary to develop a consent template for the processing of personal data and a pattern for withdrawal of consent to the processing of personal data.

4.3.9 Develop a data leakage reporting procedures and templates

The GDPR introduces a new obligation for administrators and processors of personal data to report violations of data security directly to the Supervisory Authority.
In this regard, it may be the destruction, loss, alteration or unauthorized disclosure of personal data that should not have occurred.
In the event of a higher risk to data subjects, these persons must be informed of the breach. If there is any doubt as to whether this risk exists, it is recommended to report it. All the employees were instructed to report a data leakage within 72 hours. As part of the work, reporting templates to DPA and to data subject were developed.

4.3.10 Introduce internal regulations

As part of the project for the introduction of the GDPR at the enterprise, the need to introduce internal regulations which relate to different areas of the hotel's activities regarding the processing, storage, protection and disposal of personal data was established. For the development and introduction of internal regulations, author used document templates which were revised and adjusted by the author accordingly. This chapter will examine the substantive aspects of these documents.

4.3.10.1 Privacy Policy

This document is laying down rules on the safety of personal data under the GDPR. It consists of several provisions explaining the key aspects of the protection of personal data in the context of this enterprise:

- Introductory provisions
- Interpretation of terms

  This chapter explains the basic terms in the field of the GDPR, such as organization, data controller, authorized person, supervisory authority, security incident etc.
- General conditions

  In this part the general conditions are explained. It describes the obligations of employees, legal status of the organization, as well as the interaction in the case of inter-company contractual data processing
- Personal security

  This chapter explains rights and obligations of employee and organization during the staff selection procedure and employment, also it describes personal security requirements.
- Organizational security

  This provision regulates the organizational aspects of access to the data and the internal rules of data processing and storage.
- Technical safety

  It describes technical measures to prevent data leaks, the regulation of access and data protection in the IT -related part of this enterprise, written and electronic data storage organization.
- Incident reporting.

  This part describes the basic conditions and actions of employees in case of data leakage, as well as the main legislative provisions that guide the enterprise in this area.
- Final Provisions

  It concludes all provisions, obliges the responsible persons to periodically check the security status of the data protection/processing organization in the hotel.

4.3.10.2 Personal Data Protection Directive

This document sets out the principles of the protection of personal data, including the principles of protection of facilities and the means of processing of personal data. This document consists of the following provisions:

- Introductory provisions
- Interpretation of terms

  This chapter explains the basic terms, such as organization, information, sensitive personal data, processing, principles of personal data processing etc.
- General conditions

  This part describes the legal status of an enterprise in relation to the processing of personal data, the obligations of employees to comply with the GDPR, regulates relations in the case of contractual processing of personal data by another enterprise, and also establishes obligations for the protection of personal data from unauthorized access, storage and transfer of data by employees
- Processing principles

  This provision describes the basic principles for the processing of personal data by employees, and establishes the legal basis for processing, imposes mandatory requirements for the form, volume and manner of data processing.
- Sensitive data and processing

  This provision regulates the conditions for processing of sensitive personal data, as well as a scope of employees who have access to sensitive data processing.
- Information security

  This provision regulates the obligation of employees to maintain the security of personal data on personal devices, as well as prescribes the need for real-time protection against unauthorized access, processing and use of data. Also, this item prescribes data encryption and storage of data in specially protected places.
- Duties of executives

  This clause discloses the responsibilities of management in the field of data protection and processing. This provision establishes the responsibility of the manager to monitor and verify compliance with data security requirements, as well

as provide data to data subjects on request, and to ensure the liquidation of personal data according to the legal requirements, etc.

- Final Provisions

  This clause states that company leaders are required to periodically assess the compliance of the provisions of this Directive with the real and legal situation and to ensure a regular risk assessment in accordance with legislation.

4.3.10.3 Directive on the protection of the personal data of employees

This document is laying down the principles for the protection of the personal data of employees. This document consists of the following provisions:

- Introductory provisions

  This section explains the main purpose of this directive, which is to ensure the protection of personal data and the effective fulfillment of obligations under legal rules by employees and co-workers in organizational activities, especially when processing personal data.

- Interpretation of terms

  This article outlines the basic terms of the GDPR that are used in the text of a document, such as: organization, employee, authorized person, information, personal data, processing, processing principles, sensitive personal data, senior management.

- General conditions

  This part describes the legal status of an enterprise in relation to the processing of personal data, the obligations of employees to comply with the GDPR, regulates relations in the case of contractual processing of personal data by another enterprise, and establishes obligations for the protection of personal data from unauthorized access, storage and transfer of data by employees

- Keeping personal information about employees

  This part regulates the scope of personal data of employees that can be collected, processed and stored. It also regulates the organization's responsibilities for the processing, storage, transfer and access to personal data of employees.

- Personal Data Management of Former Employees

This article emphasizes the need for legal grounds for maintaining data on former employees and prescribes the deletion or archiving of data after the storage period or working relationship with the employee has expired.

- Information Security

  This provision regulates the obligation of employees to maintain the security of personal data on personal devices, as well as prescribes the need for real-time protection against unauthorized access, processing and use of data. Also, this item prescribes data encryption and storage of data in specially protected places.

- Duties of executives

  This clause discloses the responsibilities of management in the field of data protection and processing. This provision establishes the responsibility of the manager to monitor and verify compliance with data security requirements, as well as provide data to data subjects on request, and to ensure the liquidation of personal data according to the legal requirements, etc.

- Final Provisions

  This article points to the obligations of managers to periodically assess the compliance of the provisions of this document with the real and legal status and to ensure regular risk assessment in accordance with legal regulations.

4.3.10.4 Directive on the processing of sensitive data and personal data of children

This Directive is laying down the principles for the protection of sensitive personal data, including the personal data of children. This document consists of the following provisions:

- Introductory provisions

  This section explains the main purpose of this directive, which is to ensure the protection of personal data and the effective fulfillment of obligations under legal rules by employees and co-workers in organizational activities, especially when processing personal data.

- Interpretation of terms

  This article outlines the basic terms of the GDPR that are used in the text of a document, such as: organization, employee, authorized person, information,

personal data, processing, processing principles, sensitive personal data, school, juvenile, child, manager.

- General conditions

  This part describes the legal status of an enterprise in relation to the processing of personal data, the obligations of employees to comply with the GDPR, regulates relations in the case of contractual processing of personal data by another enterprise, and establishes obligations for the protection of personal data from unauthorized access, storage and transfer of data by employees

- Sensitive data and its processing

  This article describes the conditions under which sensitive personal data can be processed and determines the scope of persons who can process data. This article also indicates types of sensitive data that are not subject to processing. This article emphasizes the need to establish a mechanism for determining the age in the processing of personal data of children and describes situations in which consent is needed for the processing of personal data of children.

- Duties of executives

  This article describes the responsibilities of a manager, keeping records of sensitive data processing, updating reports, and once every six months, conducting a compatibility check with the law.

- Final provisions

  This article points to the obligations of managers to periodically assess the compliance of the provisions of this document with the real and legal status and to ensure regular risk assessment in accordance with legal regulations.

4.3.10.5 Supervision and Privacy Guidelines

This document is laying down a company's approach to a procedure of the supervision and control conducted by the supervisory authority in the field of personal data protection
This document contains the following provisions:

- Introductory provisions

  This paragraph describes the main purpose of this document, which is to regulate the organization's activities during inspections by the supervisory authority.

- Interpretation of terms.

This provision describes the basic terms used in the document, such as: organization, employee, information, personal data, processing, processing principles and supervisory authority.

- General conditions

  This provision establishes the legal status of an organization in relation to the processing of personal data, as well as it obliges employees to assist in every way during inspections by the supervising authority. The provision also obliges employees to comply with all paragraphs of the document and explains the rules for storing and archiving all documents coming from regulatory authorities. The article obliges managers to exercise control over the implementation of this directive and explains the procedure for interaction with regulatory authorities.

- Providing information to the Supervisory Authority

  This paragraph discloses the scope and types of information that the organization undertakes to provide to the supervisory authority, as well as establishes the procedure for transmitting and processing requests from regulatory authorities.

- Audit by the Supervisory Authority

  This paragraph discloses the powers of the supervisory authority during the audit, as well as the duties of the staff in assisting in the conduct of the audit and the preparation of relevant documentation and reports.

- Notice of breach of obligations

  This article describes the procedures in case of violations identified, and the duties of responsible staff to eliminate them within a certain period.

- Regulation of the Supervisory Authority

  This article describes the procedure for interacting with the supervisory authority if recommendations or direct instructions were received. It includes procedures for their implementation and timeframes, as well as identifies the responsibilities of responsible persons for the execution of instructions of the authorities.

- Remedies and fines

  This item requires employees to use all possible corrective measures, as well as obliges to inform the manager about the imposition of a fine by the supervisory authority and prescribes its timely payment by the organization.

- Final Provisions

This item requires managers to periodically assess the compliance of the provisions of the Directive with the real and legal status and to ensure regular risk assessment in accordance with legal regulations.

4.3.10.6 Data Protection Officer Policy

This Directive is about appointees for the protection of personal data. This document consists of the following provisions:

- Introductory provisions

  This part describes the main purpose of this document, which is to define the role of Data Protection Officer in a company.

- Interpretation of terms

  This section emphasizes the basic terms used in this document, such as: organization, employee, Data Protection Officer, information, personal data, processing, supervisory authority.

- General conditions

  This part determines the legal status of the organization in relation to data processing, also defines the duties of employees to comply with the provisions of this document and other internal documents of the enterprise. It also indicates that the company assigns DPO, which is responsible for all the operations for processing of personal data at the company.

- Personnel occupation of DPO

  This part describes the criteria for the appointment of the DPO, determines the scope of the people to be appointed to the position. In addition, this article describes the procedure of employment, as well as the obligations of the newly established DPO to comply with all internal rules and directives of the company.

- Organizational rules

  This article describes the organizational rules that relate to the DPO: the order of subordination, the provision of necessary information by the organization, as well as the procedure for expanding the staff and the formation of the DPO team if needed.

- Tasks of DPO

This section establishes the tasks that the DPO must perform, as well as the principles and order of execution of the tasks. Additional tasks are also described, as well as indicated the fact that sanctions cannot be applied to the DPO in the case of direct duties performance.

- DPO involvement in organization activity

  This provision requires DPO to be involved in the work of the enterprise, in particular to be present at organizational events, to provide an opinion on the processing and protection of data, etc. As well as instructs employees on all matters relating to personal data to contact DPO and provide the necessary assistance in the implementation of its activities.

- Providing information

  This section prescribes the placement of DPO contact details on the organization's website as well as their distribution within the organization and their submission to the supervisory authority.

- Final Provisions

  This article obliges DPO and management to periodically assess the compliance of the provisions of this Directive with the real and legal status and ensure the compliance with the legislation and evaluate the effectiveness of the technical and organizational measures introduced by this Directive.

4.3.10.7 Closed Circuit Television Directive

This Directive is about the establishment of basic rules for the operation of video surveillance systems. This document consists of the following provisions:

- Introductory provisions

  This provision describes the main purpose of the document which is to create internal rules for the effective operation of camera systems and to fulfill obligations in the field of personal data processing by employees using camera systems.

- Interpretation of terms

  This part describes the basic terms used in the document, such as organization, employee, video surveillance systems, information, personal data, processing, processing principles, DPO, and so on.

- General provisions

This part determines the legal status of the organization in relation to data processing, also defines the duties of employees to comply with the provisions of this document and other internal documents of the enterprise. It Explains in which cases the term “data processing” is applicable to video surveillance systems, as well as in which cases the data from the cameras may relate to personal data. It also describes the obligations of the parties when providing surveillance cameras on the basis of contractual relations.

- The basic rules for the operation of video surveillance systems in organizations

  This article describes the basic rules for the operation of video surveillance systems, establishes the basic principles of operation, prescribes the rules for storing, use and deletion of recorded data.

- Creating a camera system

  This provision describes the actions and responsibilities of the parties when creating a surveillance camera system. In particular: Creation of project documentation, the procedure for approving or rejecting a project, the obligation of the DPO in terms of analyzing the consequences of installing cameras.

- Camera System Documentation

  This provision discloses the person responsible for maintaining records regarding video surveillance systems, as well as the scope of information that should be included in the documentation. The provision also indicates the responsibility of a person regarding the relevance of the documentation and the obligation to provide documentation upon request to authorized persons.

- Use of records

  This article reveals the use of camera system records, the responsibility of people using data, as well as the procedure for storing, copying, and deleting of data.

- Informing of data subjects

  This provision discloses the company's responsibilities regarding informing guests about video surveillance. It describes the procedure and form of performance of the responsibility, as well as emphasizes the procedure for providing information on video surveillance for data subjects.

- Security of video surveillance systems

This provision describes the company's security guarantees for the video surveillance system and the recorded data.

- Final provisions

  This article obliges management to periodically assess the compliance of the provisions of this Directive with the real and legal status and ensure the compliance with the legislation and evaluate the effectiveness of the technical and organizational measures introduced by this Directive.

4.3.10.8 Revocation Guidelines and Processing Restrictions

This paper deals with the withdrawal of the consent and other restrictions on the processing of personal data. The document consists of the following provisions:

- Introductory provisions

  This provision explains the purpose of this document, which is to define the basic rules and procedures in case of withdrawal of consent or restrictions on the processing of personal data.

- Interpretation of terms

  This chapter describes the basic terminology used in this directive, it includes such concepts as: organization, employee, responsible person, information, processing, Supervisory Authority, consent, restriction on processing.

- General conditions

  This chapter describes the legal status of an organization in relation to the processing of personal data, as well as the duties of employees and people responsible for the processing of personal data.

- Revocation of consent

  This article describes the company's obligations to exercise the right of withdrawal of consent by the data subject, and also establishes possible ways to withdraw consent for the processing of personal data. The provision also indicates the need to verify the identity of the caller, and also emphasizes the fact that the withdrawal of consent may be associated with financial expenditure of the data subject.

- Procedure for withdrawal of consent

  This provision describes the procedure for withdrawal of consent, and the duties of employees to identify the data subject and establishes the rules for interaction with

withdrawal of consent. The provision clarifies the procedure and conditions for deleting and anonymizing data and indicates the scope of responsible persons. In addition, the procedure for informing the data subject about the outcome of the withdrawn consent is described.

- Restrictions on the processing of personal data

  This provision describes cases in which the processing of personal data is prohibited and explains exceptions to the abovementioned rule. In addition, the conditions are given, under which a personal data processing prohibition arises, such as: a request from a data subject, or the company's performance of its legal duties.

- Procedure for limiting the processing of personal data

  This article describes the procedure for restricting the processing of personal data. It explains the procedure for submitting requests by the data subject, as well as the procedure for the execution of the request by the responsible officer.

- Other processing restrictions

  This provision describes the duty of the responsible officer to control the legitimacy of all requests for restriction on data processing in the case of receiving requests not stipulated by the provision.

- Personal data processors

  This provision discloses the duties of data processors if the data is processed by a third-party organization, as well as their obligations regarding the restriction or prohibition of data processing.

- Final Provisions

  This clause obliges the responsible persons to periodically check the compliance of this document with legal norms, as well as to check its implementation.

4.3.10.9 Policy on the Rights of Data Subjects

This paper deals with the withdrawal of the consent and other restrictions on the processing of personal data. The document consists of the following provisions:

- Introductory provisions

This provision explains the purpose of this document, which is to define the basic rules and procedures in case of withdrawal of consent or restrictions on the processing of personal data.

- Interpretation of terms

  This chapter describes the basic terminology used in this directive, it includes such concepts as: organization, employee, responsible person, information, processing, Supervisory Authority, consent, restriction on processing.

- General conditions

  This chapter describes the legal status of an organization in relation to the processing of personal data, as well as the duties of employees and people responsible for the processing of personal data.

- Revocation of consent

  This article describes the company's obligations to exercise the right of withdrawal of consent by the data subject and establishes possible ways to withdraw consent for the processing of personal data. The provision also indicates the need to verify the identity of the caller and emphasizes the fact that the withdrawal of consent may be associated with financial expenditure of the data subject.

- Procedure for withdrawal of consent

  This provision describes the procedure for withdrawal of consent, and the duties of employees to identify the data subject and establishes the rules for interaction with withdrawal of consent. The provision clarifies the procedure and conditions for deleting and anonymizing data and indicates the scope of responsible persons. In addition, the procedure for informing the data subject about the outcome of the withdrawn consent is described.

- Restrictions on the processing of personal data

  This provision describes cases in which the processing of personal data is prohibited and explains exceptions to the abovementioned rule. In addition, the conditions are given, under which a personal data processing prohibition arises, such as: a request from a data subject, or the company’s performance of its legal duties.

- Procedure for limiting the processing of personal data

This article describes the procedure for restricting the processing of personal data. It explains the procedure for submitting requests by the data subject, as well as the procedure for the execution of the request by the responsible officer.

- Other processing restrictions
  This provision describes the duty of the responsible officer to control the legitimacy of all requests for restriction on data processing in the case of receiving requests not stipulated by the provision.
- Personal data processors
  This provision discloses the duties of data processors if the data is processed by a third-party organization, as well as their obligations regarding the restriction or prohibition of data processing.
- Final Provisions
  This clause obliges the responsible persons to periodically check the compliance of this document with legal norms, as well as to check its implementation.

4.3.11 Conduct employee training

It is vital that all employees know about the GDPR and its main provisions. In the context of this thesis the training was conducted by the researcher personally. The following topics were covered:

- Introduction to training;
- Security of Personal Data;
- Privacy, including processing facilities;
- Data subjects' rights;
- Revocation of consent and other limitations on the processing of personal data;
- Processing of sensitive personal data and children's personal data;
- Personal Data Protection of Employees;
- Camera systems;
- Personal Data Protection Officer;
- Supervision and control of the protection of personal data.

Upon completion, each employee signed confirmation of completion of the training. This document includes a protocol of the training and statement regarding the completion of the course.

4.3.12 Develop a control mechanism

It is necessary to develop a control mechanism that will focus on the data processing operations within the organization, to make sure that no errors occurred, and there is no risk for the company connected with the data processing violations.

The company's documents require management to conduct the regular check of the data processing at least every 6 months, but it was decided to make checks on a monthly basis during the first week of each month.

Name and Surname	Scope of the data processed	Legal basis for the data processing	Terms of the storage	Form of the data	Place of storage	Deletion date	Date of the control	Controller's comments

Table 5 - Control mechanism checklist

Source: own work (2019)

The abovementioned Table 5 sets out requirements that the control of the personal data processing system should include. The reviewer will select 20 random hotel guests and evaluate the correctness of the use and storage of data. Points to be monitored:

- Check whether the company handles only the data that is actually needed for processing purposes (data minimization);
- Check legal grounds for receiving and processing data;
- Check the retention and deletion of data, check with the system, whether the appropriate data has been deleted;
- Check the form of documents and storage conditions, check whether the conditions are met, and all data are properly stored;
- Leave a comment on the correct /incorrect usage and storage of personal data or regarding additional violations that are not included in the checklist.

4.4 Project evaluation

The aim of the project was to implement the GDPR in the given hotel enterprise. The preparation and implementation of the GDPR entails certain risks and cost loads, so there is made an attempt to evaluate them using certain methodologies.

4.4.1 Risk analysis

For the evaluation of the GDPR implementation project's risks it was decided to use an approach developed by the Centre for Information Policy Leadership (Hunton & Williams LLP) as a framework to CIPL GDPR Interpretation and Implementation Project which defines certain concepts and methods of risk assessment in the context of the GDPR (Centre for Information Policy Leadership (Hunton & Williams LLP), 2016). For the needs of risk assessment, CIPL Risk Matrix was updated to best match needs of the hotel, the risk is evaluated in three components, with respect to the probability of occurrence,(A) the severity of the consequence(B) and the opinion of the evaluators(C). For all three ranges, the scale was increased from 1 to 5. Multiplying these three values generates the total risk value(D). The individual risk rates are then as follows:

- insignificant risk (<3);
- acceptable risk (3-10);
- mild risk (11-50);
- undesirable risk (51-99);
- unacceptable risk (100+).

Risk assessment is presented in Table 6:

Type of activity	Source of risk	Identification of threats	Risk Rating				Security measures
GDPR Implementation			A	B	C	D	
	Sanctions	Time delay in GDPR implementation	4	5	5	100	Necessary to implement all the provisions of GDPR as soon as possible.

	Incorrect implementation	Badly defined processing purposes	3	3	3	27	Comprehensive study of requirements
	Personal Data Leakage	Unskilled Employees	2	3	3	18	Employee training

Table 6 - Risk assessment

Source: Centre for Information Policy Leadership (Hunton & Williams LLP), (2016), own calculations (2019)

In accordance with the analysis performed, it becomes obvious that there was an imminent risk of sanctions due to the fact that at the time of the commencement of this work the hotel was not ready for the GDPR, despite the fact that a large amount of time had passed since its adoption. The hotel was still not checked by the regulatory authority and no penalty was imposed, but this was only a matter of time. This required the expedited implementation of adequate risk mitigation measures to an acceptable level, and the necessary resources had to be allocated to reduce the risk. In order to eliminate the risk, it was necessary to implement GDPR in the hotel as soon as possible.

Another risk was connected to the incorrect implementation of GDPR and hence the imminent sanction due to the poor understanding of the principles of the General Data Protection Regulation. It was important to thoroughly study all the principles and requirements, or to undergo training on the GDPR.

4.4.2 Project cost calculation

This project was made in view of minimizing the cost of implementing the GDPR. A lion's share of the work on the implementation of the GDPR was done by the author, so the company did not incur expenses for the author’s work, however, expenses appeared in other areas. The company also did not incur expenses for updating the web site and updating the electronic data processing system, since it has a personal IT specialist, who performed all the necessary manipulations as part of his job duties. In addition, the hotel did not need to consult with lawyers and specialists of the GDPR, since the work and implementation plan were realized by the author personally.

Thus, the costs of implementing the GDPR were grouped into the Table 7:

Expenses category	Amount
30 flash drives with encryption software	4770 CZK
A magnetic lock for archive door	1550 CZK
Data Protection Officer (monthly)	8000 CZK
Camera Images	1000 CZK
Employee Training working hours compensation	10168 CZK
Total	25488 CZK

Table 7 - GDPR implementation costs calculation

Source: own work (2019)

The total cost of this project is estimated at 25488 CZK with the monthly recurring costs of 8000 CZK for DPO services.

4.5 The impact of the introduction of the GDPR on the hotel activities

Considering the fact that few months has passed since GDPR was implemented at the chosen company, we can already assess its impact. In the framework of the assessment it was decided to conduct a cross-survey among guests, employees, and hotel management in order to identify the impact of the introduction of the GDPR on the hotel activities Special questionnaires were developed for each category of people, as the survey was completed, the results of were analyzed and the results were provided.

4.5.1 Guests

Since the hotel has no right to disclose personal data to third parties, it was decided to conduct an anonymous research on each case of the treatment of data subjects on the exercise of their rights. As soon as the hotel received a request to conduct any operations with personal data of data subjects, data subjects were asked to undergo an anonymous survey together with the received response to the request. If the answer was received in electronic form, the email contained a special form to fill out, the paper response also contained a printed survey version with a request to fill in and send to the hotel email. This survey has two goals: to evaluate the effectiveness of the implemented GDPR project, and to find out the opinion of guests about whether the GDPR affected the hotel service. The survey template can be found in the Appendix 3.

The hotel received 8 responses to this questionnaire. Results are grouped into the Table 8:

Questions:	Answers & number of respondents			
Are you aware of the GDPR?	Yes		No	
	8		0	
How would you rate your level of knowledge of the GDPR?	Low	Medium	High	
	2	5	1	
Did you exercise your rights in the context of the GDPR?	Yes		No	
	8		0	
What right was exercised?	Right to erasure		Right to rectification	
	6		2	
Request submission form:	Paper		Electronic	
	2		6	
How many days did it take from the day of the request to receive a response?	15 days	14 days	12 days	
	3	4	1	
Was the request satisfied?	Yes		No	
	2		6	
If no, please specify the reason described in the response to the request.	Hotel has to fulfill its legal obligation and store data for a certain period of time.			
Are you satisfied with the hotel performance of GDPR rules?	Yes		No	
	5		3	
What is your attitude towards the GDPR?	Positive	Neutral	Negative	
	6	2	0	
Did the introduction of the GDPR negatively influenced the level of hotel service?	Yes		No	
	0		8	
How many times have you been at Hotel Royal Prague?	1	2	3	More
	2	4	1	1

Table 8 - Survey results (guests)

Source: own work (2019)

For 6 of the guests interviewed, this was not the first trip to the hotel, according to a survey, 8 of respondents answered that the level of hotel service has no negative changes, since the introduction of the GDPR, thus even taking into account the fact that the hotel has become the GDPR compliant after adoption of the law.

6 of respondents sought to realize their right to erasure, and all 6 were refused, due to the fact that the hotel has to fulfill its legal obligation and store data for a certain period of time. Among all requests, only 2 were satisfied, the data subjects realized their right to rectification due to incorrect data in the hotel system, which lead to mistakes in invoicing.

6 of requests were submitted in electronic form, the rest – in paper. The average response waiting time is 14 days. Only 5 of the 8 guests surveyed were satisfied with the hotel's

work in the GDPR field. However, the author assumes that dissatisfaction with the hotel responses affected the final result.

4.5.2 Employees & Management

All employees who are associated with the processing of personal data, went through the GDPR training, and signed data processing agreements. A few months after the implementation of the GDPR project passed, and employees already had an idea of the work within the framework of the GDPR and can give a relevant input to the data. A brief anonymous questionnaire was developed to identify the impact of the GDPR on the operation of the hotel. The survey included Financial and Reservation departments, Front Office, Management, IT. The survey template can be found in the Appendix 4. A graphical interpretation of responses to the key questions of the survey will be presented in Figures 8,9,10.

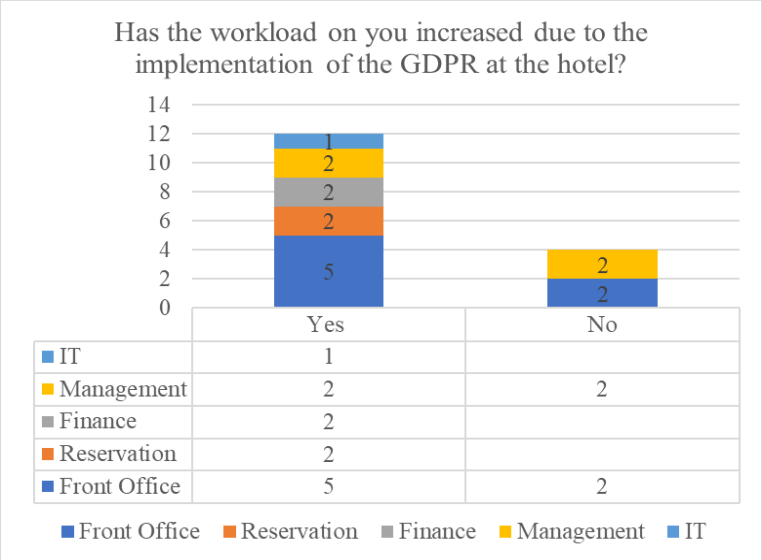

Figure 8 - Graphic representation of the answer to the survey question: Has the workload on you increased due to the implementation of the GDPR at the hotel?

Source: own work (2019)

As can be seen on the chart, the majority of respondents answered that the workload increased due to the introduction of the GDPR, mainly in all departments.

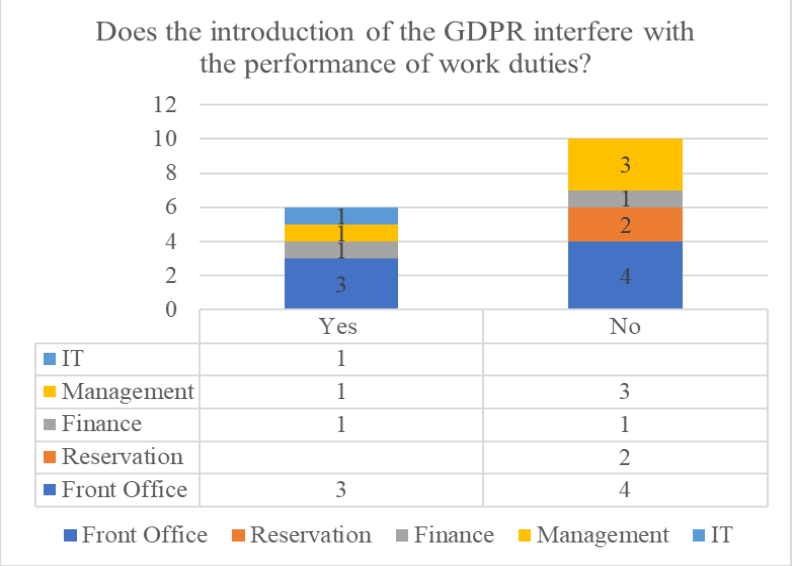

Figure 8 - Graphic representation of the answers to the survey question: Does the introduction of the GDPR interfere with the performance of work duties?

Source: own work (2019)

The chart clearly shows that more than half of employees believe that the introduction of the GDPR does not interfere with the conduct of work.

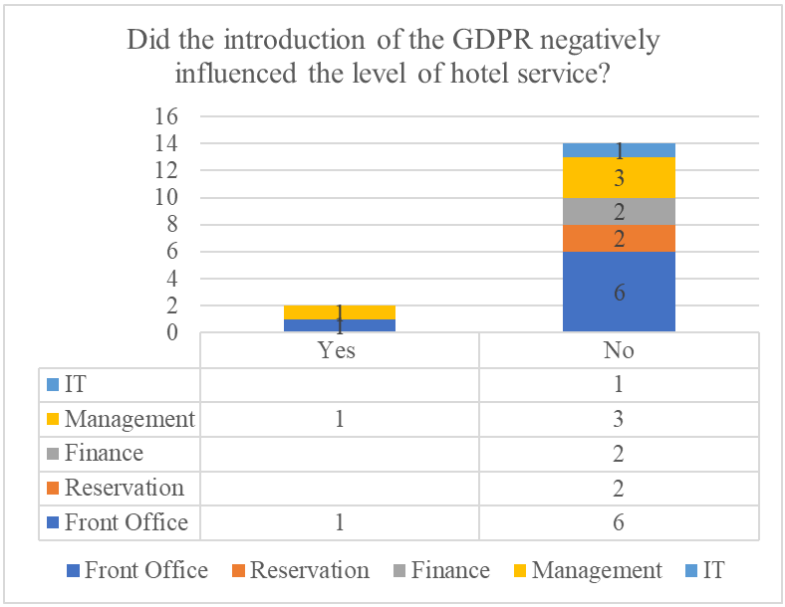

Figure 9 - Graphic representation of the answers to the survey question: Did the introduction of the GDPR negatively influenced the level of hotel service?

Source: own work (2019)

The histogram shows that the prevailing majority of employees believe that the GDPR does not affect the service level of the hotel.

In addition, 100% of the staff responded that the introduction of the GDPR had no effect on the level of their salaries.

4.5.3 Management

The author conducted a survey on the influence of the GDPR on the economics of the hotel business. The respondents were hotel managers. This category was chosen because it is relevant for issues related to the economic and organizational indicators of the hotel. A questionnaire was compiled regarding the above topic, it can be found in the Appendix 5 There are 4 respondents in total.

100% of respondents believe that the introduction of the GDPR in no way affects the pricing, revenue, and the number of hotel guests.

However, 100% of respondents are confident that the introduction of the GDPP brought costs.

An attempt is made below to analyze the influence of the GDPR on the change in hotel prices, the number of guests, and costs, thus, confirming or disproving management considerations on this matter.

One month of the hotel activity before the introduction of the GDPR, as well as the corresponding period after the introduction of the GDPR were taken for comparison and grouped in the Table 9:

	November 2017	November 2018
Average price per night	118.3 EUR	118.4 EUR
Average monthly occupancy	57.5%	58.7%
Monthly costs	76979 EUR	81979 EUR
Monthly revenue	312567 EUR	322166 EUR

Table 9 - Comparison of economic indicators of the hotel before the introduction of the GDPR and after

Source: Hotel management data, own work (2019)

In accordance with the table, it is seen that the average price per night, as well as the average monthly occupancy, does not indicate any significant changes. In turn, there are noticeable changes in revenues and costs, however, as indicated above, this is a

consequence of the opening of the restaurant, and the introduction of the GDPR on an ongoing basis includes only the monthly expenses for the payment to DPO.

Thus, the above analysis confirms the results of a survey among hotel management.

5 Results and Discussion

This work focuses on the impact of the introduction of the GDPR on the business on the example of a hotel.

Based on the study, it became clear that:

- Introduction GDPR did not imply the level of service at the hotel and customer satisfaction.
- The introduction of the GDPR increased the workload of the hotel staff.
- GDPR in no way affected the level of revenue of the hotel and the number of guests.
- Spending on GDPR stated 25 thousand crowns, which is an uncompromisingly small amount in relation to the hotel's profit, but its introduction resulted in constant hotel spending, which is reflected in regular payments to the DPO.

In order to understand how far the obtained results, correspond to business and statistical reality, it was decided to conduct a survey among companies that are engaged in the same type of business activity. In the vicinity of the hotel there are several other hospitality businesses, on the basis of which the survey was conducted. Surveys were conducted in two neighboring hotels of the similar level of service and size. Only the enterprise management was surveyed. The questionnaire is based on internal client, management and staff surveys, which were assembled and revised in Appendix 6.

Both hotels agreed on the fact that the introduction of the GDPR did not affect the quality of hotel services. It was responded that the GDPR implementation partially increased the work burden on hotel staff and did not affect the level of revenue and number of guests.

The first hotel spent on the introduction of the GDPR 70,000 crowns, at the same time, the cost of GDPR implementation of another hotel was 58,000. According to the data of the company Česká Síť, which provides services in the field of the GDPR in the Czech Republic, the cost of the GDPR implementation is calculated individually, but for large enterprises or hotels it can be about 60,000 crowns (Česká síť, s.r.o., 2018), while the Czech Chamber of Commerce estimates the average spending on the introduction of the GDPR at 50,000 CZK (Globe24.cz / ČTK, 2018). As it is seen from the above results, the neighboring hotels spent on the introduction of the GDPR considerably more resources. This is explained by the fact that for the introduction of the GDPR hotels used consultations and services of third-party companies. And the cost of these services

amounted to about 90% of the cost of the entire GDPR implementation project. In the case of the Hotel Royal Prague, all the advisory services were provided by the author personally, and internal documents and trainings were presented as well. Thus, there were no additional costs that would lead to an increase in the cost of the project. However, it is worth noting that even amounts of 70,000 or 57,000 crowns are not a heavy burden for hotels of this size.

6 Conclusion

The main objective of this work was to study the influence of the GDPR on business. As part of this work, the background to the introduction of the GDPR in the European Union, the main reasons for the transition to the GDPR, as well as the main innovations of this law in the context of the rights and obligations of the parties were studied.

The main controversial issues of the GDPR in relation to modern technologies, business and ordinary citizens were studied, and potential consequences were identified.

In order to empirically study the impact of the introduction of the GDPR on a business, an implementation project has been developed and realized to introduce the GDPR on an example of hospitality industry. Within the framework of the project, a full-fledged plan for the introduction of the GDPR in the selected business was developed and implemented, the risks were assessed, and the costs were calculated. In addition, the impact of the introduction of the GDPR on hotel income, expenses, level of service and number of guests was analyzed.

The results obtained during the research confirm the relevance of the selected topic, and realized objectives give the opportunity to make following conclusions:

- The introduction of the GDPR inevitably leads to an increase in bureaucratization and control in the business processes. This is primarily applicable to the hotel business, since in some cases there is a need to collect consents about the processing of personal data from data subjects, which leads to an increase in paperwork. The implementation of the rights of citizens in the context of the GDPR requires additional paperwork and staff efforts. The number of necessary internal orders, norms and rules that complicate business interaction has been increased. In addition, in the case of transferring the data processed to third parties, the procedure is complicated by the need to sign special agreements on the processing of personal data and receive guarantees from a third party that this data is safe.
- The implementation of the GDPR rules lead to tangible increase in the workload on employees working with data, which sometimes interferes with business processes. This is a consequence of the preceding paragraph, since staff need to fulfill not only their direct duties, but also additionally perform duties prescribed by the norms of the GDPR.

- The cost of the introduction of the GDPR can be burdensome for the small businesses. The cost of introducing an GDPR in a business varies depending on the type of activity and the amount of personal data that the business collects. In the case of a large hotel, the costs amounted to a very small fraction of its income, but if we consider, for example, a small online store, one-time investment of fifty thousand CZK can have a very negative impact on the business.
- A large scale of possible fines can hit GDPR-incompliant business hard. The maximum fine for violation of GDPR norms is up to 20 million EUR, or 4% of the violator's turnover, which is a very heavy sum for small and medium businesses. For the sake of justice, it is worth noting that each case of violation of the GDRP is considered individually, and the party that violates the rules may not incur the maximum penalty, escaping with a smaller amount or non-monetary penalties.
- Extensive and not always clear wording in the law and the lack of a clear procedure for GDPR introduction complicates the process of applying the GDPR. The consequence of this clause is that the business seeks to hire external consultants in order to comply with the standards of the GDPR, since without professional advice it is very difficult to apply the GDPR in the company. In addition, in spite of the fact that the GDPR is a unified European law, there is space for action for local Supervisory Authorities that can interpret the law slightly differently depending on local peculiarities.
- The introduction of the GDPR did not affect the revenue, number of guests and the level of service in the hospitality industry. According to the study, there were no significant changes in the income, expenses, or number of hotel guests after the introduction of the GDPR. The introduction of the GDPR in the hotel resulted in an increase in expenses for DPO services, as well as a one-time investment for GDPR implementation project.

Thus, the GDPR, by setting itself the task of protecting the personal data of citizens, complicates the conduct of a business in the European Union, however these are time norms that must be considered, and positive changes in the rights of European citizens, worthy of the price paid by companies for being GDPR-compliant.

7 References

Askari, Fes. 2018. GDPR And Digital Marketing: What Do You Need To Know? *Online Marketing Institute Web site.* [Online] May 18, 2018. [Cited: February 24, 2019.] https://www.onlinemarketinginstitute.org/blog/2018/05/GDPR-digital-marketing-need-know/.

Bazanov, Sergey. 2017. Биткоин за 5 минут: Блок. *Bitcoin Review.* [Online] June 28, 2017. [Cited: February 24, 2019.] https://medium.com/bitcoin-review/%D0%B1%D0%B8%D1%82%D0%BA%D0%BE%D0%B8%D0%BD-%D0%B7%D0%B0-5-%D0%BC%D0%B8%D0%BD%D1%83%D1%82-%D0%B1%D0%BB%D0%BE%D0%BA-321984df178c.

Centre for Information Policy Leadership (Hunton & Williams LLP). 2016. Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. *Centre for Information Policy Leadership (Hunton & Williams LLP) Web site.* [Online] December 21, 2016. [Cited: February 24, 2019.] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

Česká síť, s.r.o. 2018. Kolik stojí zavedení GDPR? *Česká síť, s.r.o. Web site.* [Online] June 2, 2018. [Cited: February 24, 2019.] https://www.ceskasit.cz/kolik-stoji-zavedeni-gdpr/.

Council of Europe. 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *Council of Europe Web site.* [Online] January 28, 1981. [Cited: January 24, 2019.] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

Court of Justice of the European Union. 2015. Judgment in Case C-230/14. *Court of Justice of the European Union.* [Online] October 1, 2015. [Cited: February 24, 2019.] https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150111en.pdf.

European Commission. 2010. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union". *EUR-Lex. Access to European Union law.* [Online] April 4, 2010. [Cited: February 25, 2019.] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52010DC0609.

European Court of Human Rights, Council of Europe. 1950. The Convention for the Protection of Human Rights and Fundamental Freedoms. *Council of Europe Web site.* [Online] November 4, 1950. [Cited: January 24, 2019.] https://www.echr.coe.int/Documents/Collection_Convention_1950_ENG.pdf.

European Court of Justice. 2014. Judgment of the Court (Grand Chamber), 13 May 2014.Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. *EUR-Lex. Access to European Union law.* [Online]

May 13, 2014. [Cited: February 24, 2019.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

European Data Protection Supervisor. 2018. The History of the General Data Protection Regulation. *European Data Protection Supervisor Web site.* [Online] 2018. [Cited: February 24, 2019.] https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

European Parliament, The Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. *EUR-Lex. Access to European Union law.* [Online] April 2016, 2016. [Cited: February 24, 2019.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Forbes Technology Council. 2018. 15 Unexpected Consequences Of GDPR. *Forbes Web site.* [Online] August 15, 2018. [Cited: February 24, 2019.] https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#45bbf69894ad.

Globe24.cz / ČTK. 2018. Náklady firem na GDPR? 25 miliard, tvrdí Hospodářská komora. *Globe24.cz.* [Online] May 24, 2018. [Cited: February 24, 2019.] https://globe24.cz/domov/56236-naklady-firem-na-gdpr-25-miliard-tvrdi-hospodarska-komora.

Information Commissioner's Office. 2017. ICO GDPR guidance: Contracts and liabilities between controllers and processors. *Information Commissioner's Office Web Site.* [Online] September 13, 2017. [Cited: February 24, 2019.] https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf.

Januš, Jan. 2018. Kolik GDPR stálo firmy? Ty středně velké i stovky tisíc korun, říkají právníci. *Info.cz.* [Online] May 30, 2018. [Cited: January 1, 2019.] https://www.info.cz/pravo/kolik-gdpr-stalo-firmy-ty-stredne-velke-i-stovky-tisic-korun-rikaji-pravnici-31126.html.

Jeremy Kahn, Stephanie Bodoni, Stefan Nicola. 2018. It'll Cost Billions for Companies to Comply with Europe's New Data Law. *Bloomberg Web site.* [Online] March 22, 2018. [Cited: February 24, 2019.] https://www.bloomberg.com/businessweek.

Lima, Claudio. 2018. Adapting Blockchain for GDPR Compliance. *InformationWeek* . [Online] July 8, 2018. [Cited: February 24, 2019.] https://www.informationweek.com/strategic-cio/security-and-risk-strategy/adapting-blockchain-for-GDPR-compliance-/a/d-id/1332499.

Lyons, Lucy. 2016. Enforcement and sanctions under the GDPR. *Taylor Wessing. Global Data Hub.* [Online] April 2016. [Cited: January 5, 2019.]

https://globaldatahub.taylorwessing.com/article/enforcement-and-sanctions-under-the-gdpr.

Neil Robinson, Hans Graux,Maarten Botterman, Lorenzo Valeri. 2009. Review of the European Data Protection Directive. *ICO. Information Commissioner's Office Web site.* [Online] May 2009. [Cited: January 24, 2019.] https://ico.org.uk/media/1042349/review-of-eu-dp-directive.pdf.

Ponemon Institute LLC. 2017. The true cost of compliance with data protection regulations. *Globalscape Web site.* [Online] December 2017. [Cited: February 24, 2019.] https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf.

Privacy and Data Security Practice Group. 2016. EU Advocate General Considers Dynamic IP Addresses To Be Personal Data. *The National Law Review* . [Online] May 13, 2016. [Cited: February 24, 2019.] https://www.natlawreview.com/article/eu-advocate-general-considers-dynamic-ip-addresses-to-be-personal-data.

Privacy Laws & Business. 2018. First significant GDPR fines in the pipeline. *Privacy Laws & Business Web site.* [Online] October 17, 2018. [Cited: January 1, 2019.] https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2018/10/First-significant-GDPR-fines-in-the-pipeline/.

Rouse, Margaret. 2008. EU Data Protection Directive (Directive 95/46/EC). *TechTarget Web site.* [Online] January 2008. [Cited: 02 24, 2019.] https://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC.

Singleton, Micah. 2016. YouTube is still having trouble getting people to pay for YouTube. *The Verge Web site.* [Online] November 2, 2016. [Cited: February 24, 2019.] https://www.theverge.com/2016/11/2/13498470/youtube-red-subscribers-video-content-music.

Stolton, Samuel. 2018. Companies may try to bypass GDPR fines by negotiating with cybercriminals, Europol say. *Euractiv Web Site.* [Online] September 20, 2018. [Cited: February 24, 2019.] https://www.euractiv.com/section/cybersecurity/news/companies-may-try-to-bypass-gdpr-fines-by-negotiating-with-cybercriminals-europol-say/.

Tolsma, Alex. 2018. GDPR and the impact on cloud computing. *Deloitte Holding B.V Web site.* [Online] n.d n.d, 2018. [Cited: February 24, 2019.] https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-GDPR-update-the-impact-on-cloud-computing.html.

Tolstov, Ellin. 2018. Собираетесь в отпуск в Европу? Вот как GDPR повлияет на вас. *Rusbase.* [Online] May 25, 2018. [Cited: January 21, 2019.] https://rb.ru/opinion/otpusk-gdpr/.

Woods, Lorna. 2015. Zakharov v Russia: Mass Surveillance and the European Court of Human Rights. *EU Law Analysis.* [Online] December 16, 2015. [Cited: January 24, 2019.] http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html.

Wright, Todd. 2018. The GDPR – Is reputation a bigger risk than fines? *SAS Web site.* [Online] January 11, 2018. [Cited: February 24, 2019.] https://blogs.sas.com/content/datamanagement/2018/01/11/gdpr-reputation-bigger-risk-fines/.

8 Appendix

8.1 Appendix 1. Analysis of personal data of hotel guests

	Category			Legal reasons (s) of processing		Purposes of processing of personal data and processing time	
Types of personal data	Categories of personal data	Sensitive?	Condition / Remark	Lawful basis for processing	Reason for selected title - reference to prescription, interest, contract, etc.	How long is personal data processed?	Purpose of processing personal information
name and surname	identification data - accounting	NO		fulfilling the statutory duty	Article 31 (2) c) of Act No. 563/1991 Coll.	5 years after the year covered by accounting documents according to the Accounting Act, 10 years of documents containing VAT	evidence of accounting documents
name and surname	identification data	NO		fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
name and surname (foreigner)	identification data	NO	in case of foreigners accommodation	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
name and surname	contractual data	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	evidence of the contractor and performance of the contract
personal identification number	contractual data	YES		performance of the contract	identification of the Contracting Party	during the validity and registration of the contract	evidence of the contractor and performance of the contract
email address	identification data - accounting	NO	if you put the email on the accounting	fulfilling the statutory duty	Article 31 (2) c) of Act No. 563/1991 Coll.	5 years after the year covered by accounting documents according to the	evidence of accounting document

			documents			Accounting Act, 10 years of documents containing VAT	s
email address	contractual data	NO		performance of the contract	contacting in performance, delivering services, delivering documents	during the validity and registration of the contract	evidence of the contractor and performance of the contract
email address	contact information	NO		legitimate interest	in case of a sudden organizational change, details of the stay, picking up a guest, bringing guests to the hotel	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	contacting a guest
address of permanent residence	identification data	NO		fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
the address of the permanent residence abroad	identification data	NO	if the guest has no permanent residence in the Czech Republic	fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
birthdate	contractual data	NO		performance of the contract	identification of the Contracting Party	during the validity and registration of the contract	evidence of the contractor and performance of the contract
date of birth (foreigner)	identification data	NO	in the case of foreigners	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
nationality (foreigner)	identification data	NO	in the case of foreigners	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
billing address	identification data - accounting	NO		fulfilling the statutory duty	Article 31 (2) c) of Act No. 563/1991 Coll.	5 years after the year covered by accounting documents according to the	evidence of accounting document

						Accounting Act, 10 years of documents containing VAT	s
accommodation time	identification data	NO	the beginning and the end are recorded	fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
accommodation time	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
accommodation time (alien)	identification data	NO	in the case of foreigners / the beginning and the end are recorded	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
purpose of stay	identification data	NO	in the case of foreigners	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
purpose of stay	identification data	YES		fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
Passport /travel document number	identification data	YES		fulfilling the statutory duty	Section 3 (4) of Act No. 565/1990 Coll., On Local Fees	for a period of 6 years after the last entry into the register	registration of guests according to the law
Passport/ travel document number	identification data	YES	in the case of foreigners	fulfilling the statutory duty	Section 101 (1) of Act No. 326/1999 Coll., On the Residence of Foreign Nationals in the Czech Republic	for a period of 6 years after the last entry into the register	registration of guests according to the law
guestbook	identification data - accommodation	NO		legitimate interest	for internal use, this legal title is appropriate	for a period of 6 years after the last entry into the register	overview and records of guests
card / hotel guest card	identification data - accommodation	NO		legitimate interest	for internal use, this legal title is appropriate	for a period of 6 years after the last entry into the register	overview and records of guests

Bank account number	identification data - accounting	NO	payment for the provided accommodation services	fulfilling the statutory duty	Article 31 (2) c) of Act No. 563/1991 Coll.	5 years after the year covered by accounting documents according to the Accounting Act, 10 years of documents containing VAT	evidence of accounting documents
Bank account number	payment information	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	records of incoming payments
credit card number / type	payment information	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	records of incoming payments
expiration date of the credit card	payment information	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	records of incoming payments
Guest ID in the external reservation system	payment information	NO	eg ID Booking.com	performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	records of incoming payments
records of previous guest stays	additional data	NO		legitimate interest	for internal use, this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
Note to reservation	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
Order Number	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time	records of stays and services

						afterwards (eg 6 months)	
reservation number	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
booking book / guest book system	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
sex	additional data	NO		legitimate interest	For hotel organizational matters this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
video recording from the camera system	safety data - record	YES		legitimate interest	for security purposes, this legal title is appropriate	maximum 14 days	security of common areas, persons and property
data about the guest's children (gender, age)	contractual data	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	evidence of the contractor and performance of the contract
specific guest requirements	additional data	YES	eating / health handicap	legitimate interest	to satisfy the guest's specific requirements, this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
Key / chips / card entry to enter the hotel and rooms	input data	NO	if the key / chip / card is issued and registered according to a specific number	legitimate interest	protection of property and persons	for the necessary duration of legitimate interest	protection of persons and property
room number and type	contractual data	NO		performance of the contract	records according to a concluded contract (Section	during the validity and registration of the contract	evidence of the contractor and

					2326 et seq. of Act No. 89/2012 Coll., Civil Code)		performance of the contract
pets	additional data	NO		legitimate interest	to satisfy the guest's specific requirements, this legal title is appropriate	for the duration of the legitimate interest and for a reasonable period of time afterwards (eg 6 months)	records of stays and services
voucher	contractual data	NO		performance of the contract	records according to a concluded contract (Section 2326 et seq. of Act No. 89/2012 Coll., Civil Code)	during the validity and registration of the contract	evidence of the contractor and performance of the contract

Appendix 1 - Analysis of personal data of hotel guests

Source: Goodking Advisory s.r.o data, own work (2019)

8.2 Appendix 2. Analysis of personal data of employees

	Category			Legal reasons (s) of processing		Purposes of processing of personal data and processing time	
Types of personal data or documents containing personal data	Categories of personal data	Sensitive	Condition / Note	legalbasisfor processing	Reason for selected title - reference to prescription, interest, contract, etc.	How long is personal data processed?	Purpose of processing personal information
name	basic personal data	NO		fulfilling the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	in order to preserve wage sheets in accordance with Section 35a (4) of the Act. 582/1991 Coll.
name	identification data of a legitimate interest	NO		legitimate interest	in favor of an employee, a legitimate interest of the employer	for the duration of the employment relationship	employee records, corporate events, teambuilding
surname	basic personal data	NO		fulfilling the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	in order to preserve wage sheets in accordance with Section 35a (4) of the Act. 582/1991 Coll.
surname	identification data of a legitimate interest	NO		legitimate interest	in favor of an employee, a legitimate interest of the employer	for the duration of the employment relationship	employee records
employment contracts - labor agreements		NO		fulfilling the statutory duty	Article 31 (2) c) of Act No. 563/1991 Coll.	5 years (after completion of the agreed work)	Article 31 (2) c) of Act No. 563/1991 Coll.

place of birth	basic personal data	NO		fulfilling the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	in order to preserve wage sheets in accordance with Section 35a (4) of the Act. 582/1991 Coll.
sex	basic personal data	NO		fulfilling the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	registration pursuant to Section 37 (1) of Act. 582/1991 Coll.
permanent residence	basic personal data	NO		fulfilling the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	registration pursuant to Section 37 (1) of Act. 582/1991 Coll.
personal identification number	basic personal data	NO		fulfilling the statutory duty	Section 37, Para. b zák.582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	in order to preserve wage sheets in accordance with Section 35a (4) of the Act. 582/1991 Coll.
employee's personal number	basic personal data	NO		fulfilling the statutory duty	keeping wage sheets in accordance with Section 35a (4) of Act. 582/1991 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	in order to preserve wage sheets in accordance with Section 35a (4) of the Act. 582/1991 Coll.
signing and unsubscribing of employees to health insurance companie	basic personal data	YES		fulfilling the statutory duty	the notification is a statutory duty within 8 days according to Act. 582/1991 Coll. and Zák.187/2006 Coll. on sickness insurance, but no	such as 5 years after the year they relate to	proof of fulfillment of the statutory obligation

s, reporting of changes					retention period is set		
reported residence of the employee (tempora ry stay)	basic personal data	NO		fulfillin g the statutory duty	evidence pursuant to Section 95 of Act 187/2006 Coll. on sickness insurance	10 years after the year they relate to	evidence pursuant to Section 95 of Act 187/2 006 Coll. on sickness insurance
nationalit y (citizensh ip)	basic personal data	NO		fulfillin g the statutory duty	the time limit under Section 35a (4) and the registration pursuant to Section 37 (1) and Zák. 582/1991 Coll.	10 years after the year they relate to	registratio n pursuant to Section 37 (1) of Act. 582/1 991 Coll.
citizenshi p of foreigner s for work permits	tax non-resident s	NO	employme nt of foreigners for work permits	fulfillin g the statutory duty	In order to report the employment of foreigners pursuant to the Employment Act No. 435/2004, Section 102, paragraph 3	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	for the purpose of reporting the employme nt of foreigners pursuant to the Employm ent Act No. 435/2004 Coll. § 87 and § 98 and § 102 and Act. No. 436/2004 Coll., on Administr ative Fees, as amended
health insurance	basic personal data 10	NO		fulfillin g the statutory duty	evidence pursuant to §96 of Act. 187/2006 Coll. on sickness insurance	10 years after the year they relate to	registratio n pursuant to Section 95 (1) i) Act. 187/2 006 Coll. on sickness insurance

Pasport number	identification data	NO	it is necessary to inform the employees	legitimate interest	legitimate interest in identifying the employee during the inspection	for the duration of the employee's need to identify	only submission of an Passport to identify whether that person is concerned
criminal record	additional data - criminal record	NO	to verify eligibility for employment	fulfilling the statutory duty	Section 30 of the Labor Code	during the employment relationship	Employee Evidence - Criminal Register
CV and personal data provided	resume legitimate interest	YES		legitimate interest	there is a legitimate interest in following the scope of qualifications	for the duration of the employment relationship	Employee Records - Curriculum Vitae
health handicap	health data	YES		fulfilling the statutory duty	pursuant to Section 81 et seq.of the Employment Act	during the employment relationship	labor law
information and education papers	personal data - education	NO	if it is a condition of a job position according to a legal regulation or it has an effect on the correct calculation of the wage	fulfilling the statutory duty	eg Government Regulation No. 341/2017 Coll.Government Regulation on the remuneration of employees in public services and administration	for the duration of the employment relationship	fulfillment of legal obligations
age	supplementary data - age	NO		legitimate interest	for an overview of the composition of the organization	for the duration of legitimate interest	such as age structure statistics
photo footage of the employee's face	identification data - photographs	YES		legitimate interest	the security checks and compares the face of the person with the photos on the entry card / the el. record in db	for the period of employment and 2 months thereafter	protective property and persons on the premises of the organization
video recording from the camera system	additional data - video recording	YES		legitimate interest	security of the organization's premises	by legitimate interest, by default within days	security of the organization's premises

mailing address	contact details - delivery address	NO		legitimate interest	eg an employee wishes to receive letters elsewhere	for the duration of the employment relationship and for example 4 years after its termination	labor law
email address - private	contact details - private	NO		legitimate interest	staffing only and in case of contact with attendance	for the duration of the employment relationship and for example one year after its termination	Employee's private e-mail records
phone number - private	contact details - private phone number	NO		legitimate interest	staffing only and in case of contact with attendance	for the duration of the employment relationship and for example one year after its termination	only for the personnel agenda and for the direct superior
Bank account number	identification data - bank account	NO	unless the wage is paid exclusively in cash	performance of the contract	if a wage is sent to a bank account	during the performance of the contract	Employee Bank Account Evidence
Health check on work (entry, periodic inspections, etc.)	health data	NO	medical records or health data are not included	fulfilling the statutory duty	Section 54 of the Law on Specific Health Services	for a reasonable period of time after the end of the employment relationship, eg 4 years	labor law
benefits	employee data - benefits	NO		legitimate interest	for the purpose, the chosen legal title is sufficient	for a reasonable period of time after the end of the employment relationship, eg 4 years	records and employee care
work or other performance	employee data - performance	NO		legitimate interest	for the purpose, the chosen legal title is sufficient	for a reasonable period of time after the end of the employment relationship, eg 4 years	records and employee care
the amount of deductible income for each payroll (payout) period and documents containing those data	basic personal data 30	NO		fulfilling the statutory duty	evidence pursuant to §96 of Act. 187/2006 Coll. on sickness insurance	30 years after the year they relate to (10 years for old-age pensioners)	evidence pursuant to Section 35a (4) of Act. 582/1991 Coll.

execution, insolvency, wage deductions, and related information	basic personal data 30	NO		fulfilling the statutory duty	Section 276 - Section 302 Civil Code No. 99/1963 Coll.	according to the wage sheet of the employee 5, 10 or 30 years after the year they relate to	Section 276 - Section 302 Civil Code No. 99/1963 Coll.
documentation on the training of employees	personal data - education	NO		legitimate interest	the employer keeps records of employee training made	for a reasonable period of time after the end of the employment relationship, eg 4 years	fulfillment of legal obligations

Appendix 2 - Analysis of personal data of employees

Source: Goodking Advisory s.r.o data, own work (2019)

8.3 Appendix 3. Survey (Guests)

1. Are you aware of the GDPR?

a) Yes b) No

2.How would you rate your level of knowledge of the GDPR?

a) Low level of knowledge b) Medium level of knowledge c) High level of knowledge

3. Did you exercise your rights in the context of the GDPR?

a) Yes a) No

4. What right was exercised?

_____

5. What was your request to the hotel?

_____

6. Request submission form:

a) Electronic b) Paper

7. How many days did it take from the day of the request to receive a response?

_____

8. Was the request satisfied?

a) Yes b) No

9. If No, please specify the reason described in the response to the request.

_____

10. Are you satisfied with the hotel performance of GDPR rules?

a) Yes b) No

11. What is your attitude towards the GDPR?

a) Positive b) Neutral c) Negative

12. Did the introduction of the GDPR negatively influenced the level of hotel service?

a) Yes b) No

13. How many times have you been at Hotel Royal Prague?

a) 1 b) 2 c) 3 d) More

Appendix 3 – Survey (Guests)

Source: own work (2019)

8.4 Appendix 4. Survey (Employees & Management)

1. Are you aware of the GDPR?

a) Yes b) No

2.How would you rate your level of knowledge of the GDPR?

a) Low level of knowledge b) Medium level of knowledge c) High level of knowledge

3. What is your attitude towards the GDPR?

a) Positive b) Neutral c) Negative

4.Were there any changes in salary due to the introduction of the GDPR?

a) Yes a) No

5.Has the workload on you increased due to the implementation of the GDPR at the hotel?

a) Yes a) No

6.Does the introduction of the GDPR interfere with the performance of work duties?

a) Yes a) No

7. Did the introduction of the GDPR negatively influenced the level of hotel service?

a) Yes b) No

Appendix 4 – Survey (Employees & Management)

Source: own work (2019)

8.5 Appendix 5. Survey (Management)

1. Are you aware of the GDPR?

a) Yes b) No

2.How would you rate your level of knowledge of the GDPR?

a) Low level of knowledge b) Medium level of knowledge c) High level of knowledge

4. What is your attitude towards the GDPR?

a) Positive b) Neutral c) Negative

5.Did the introduction of the GDPR affect hotel pricing?

a) Yes b) No

6.Were there additional costs incurred by the hotel due to the introduction of the GDPR?

a) Yes b) No

7.Did the introduction of the GDPR affect the number of guests?

a) Yes b) No

8.Did the introduction of the GDPR positively affect the amount of income received by the hotel?

a) Yes b) No

Appendix 4 – Survey (Management)

Source: own work (2019)

8.6 Appendix 6. Survey (Different Hotels)

1.Did the introduction of the GDPR affect hotel pricing?

a) Yes b) No

2.Were there additional costs incurred by the hotel due to the introduction of the GDPR?

a) Yes b) No

3.Did the introduction of the GDPR affect the number of guests?

a) Yes b) No

4.Did the introduction of the GDPR positively affect the amount of income received by the hotel?

a) Yes b) No

5. Estimate the cost of GDPR implementation in your hotel

_____

6. Did the introduction of GDPR negatively affect the level of service at the hotel?

a) Yes b) No

7. Has the burden on employees increased due to the introduction of the GDPR?

a) Yes b) No

8. How many requests were received for the execution of the rights guaranteed by the GDPR for the last 6 months?

_____

9.How many of them were satisfied?

_____

10. Do you use services of the Data Protection Officer?

a) Yes b) No

11.Did the introduction of GDPR significantly affect the budget of the hotel?

a) Yes b) No

Appendix 4 – Survey (Different Hotels)

Source: own work (2019)