Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Diploma Thesis

Analysis and impacts of GDPR in a selected organisation

Helena Daňková

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Helena Daňková

European Agrarian Diplomacy

Thesis title

Analysis and impacts of GDPR in a selected organisation

Objectives of thesis

The thesis investigates impacts of General Data Protection Regulation, the new EU legislation. The main goal of the thesis is to analyze implementation of GDPR in selected organization.

Partial goals of the thesis are such as:
- to study a current state and to make a literature review of the personal data protection framework in the European Union,
- to evaluate possible consequences of GDPR for a selected organization,
- to propose an approach to GDPR compliant data management for the given company.

Methodology

The methodology of the thesis is based on analysis of implementation of General Data Protection Regulation rules. The practical part is focused on impacts of GDPR in a selected organization. The scientific methods such as analysis, synthesis, comparison, induction and deduction will be employed. By taking qualitative and quantitative approaches, a GDPR compliant data management approach will be proposed. Based on the theoretical part and outcomes of the practical part, final recommendations will be formulated.

The proposed extent of the thesis

60 – 80 pages

Keywords

GDPR, General Data Protection Regulation, protection of personal data, ePrivacy, Data Protection Impact Assessment, CyberSecurity

---

Recommended information sources

EU general data protection regulation (GDPR): an implementation and compliance guide. IT governance privacy team. ISBN 9781849288354.

KUNER, Christopher. European data protection law: corporace compliance and regulation. 2nd ed. Oxford: Oxford University Press, 2007. ISBN 978-0-19-928385-9.

NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 8027106680.

NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 8075527658.

The EU general data protection regulation (GDPR). New York, NY: Springer Berlin Heidelberg, 2017. ISBN 9783319579580.

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: 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 24. 02. 2019

Declaration

I declare that I have worked on my diploma thesis titled "Analysis and impacts of GDPR in a selected organisation" 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 21.3.2019 _____

Acknowledgement

I would like to thank Ing. Miloš Ulman, Ph.D. and JUDr. Ing. Lukáš Pěsna, for their advice and support during my work on this thesis.

Analysis and impacts of GDPR in a selected organisation

Abstract

The thesis investigates impacts of General Data Protection Regulation, the new EU legislation. The methodology of the thesis is based on analysis of implementation of General Data Protection Regulation rules. The theoretical part describes the main properties of GDPR together with tools that help the companies to achieve GDPR compliance, like ISO 27001:2013 and ISO 31000:2018. The practical part is focused on impacts of GDPR in a selected organization. In order to assess the state of the Regulation compliance, DPIA and Risk assessment will be conduct. The scientific methods such as analysis, synthesis, comparison, induction and deduction will be employed. By taking qualitative and quantitative approaches, a GDPR compliant data management approach will be proposed. Based on the theoretical part and outcomes of the practical part, final recommendations will be formulated.

Keywords: GDPR, General Data Protection Regulation, personal data, DPIA, Data Protection Impact Assessment, Data Protection Officer, data controller, data processor, data subject, Risk Assessment

Analýza a dopady GDPR ve vybrané organizaci

Abstrakt

Závěrečná práce zkoumá dopady obecného nařízení o ochraně osobních údajů, nového právního předpisu Evropské Unie. Metodika práce vychází z analýzy implementace pravidel o obecné ochraně údajů. Teoretická část popisuje hlavní vlastnosti GDPR společně s nástroji, které pomáhají firmám dosáhnout souladu s GDPR, jako jsou ISO 27001:2013 a ISO 31000:2018. Praktická část je zaměřena na dopady GDPR ve vybrané organizaci. Aby bylo možné posoudit stav souladu s nařízením, bude provedeno DPIA a posouzení rizik. Použijí se vědecké metody, jako je analýza, syntéza, srovnání a indukce. Použitím kvalitativních a kvantitativních přístupů, bude navržen přístup GDPR pro správu dat. Na základě teoretické části a výsledků praktické části budou formulovány závěrečné doporučení.

Klíčová slova: GDPR, obecné nařízení o ochraně osobních údajů, DPIA, osobní data, posouzení vlivu na ochranu osobních údajů, pověřenec pro ochranu osobních údajů, správce dat, zpracovatel dat, analýza rizik

Table of content

List of pictures

List of tables

List of abbreviations

GDPR	General Data Protection Regulation
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
OPDP	Office for Personal Data Protection
EU	European Union
WP29	Working Party 29
EDPB	European Data Protection Board
ISMS	Information Security Management System
HTML	Hypertext Markup Language
CSS	Cascading Style Sheets
JS	Java Script
CRM	Customer-relationship management
IP	Internet Protocol
ISO	International Organization for Standardization
HW	Hardware
SW	Software

1 Introduction

General Data Protection Regulation (GDPR) represents legal framework for the protection of personal data. This regulation protects the rights of EU citizens against the unauthorized treatment of their regular and personal data. Since 25.5.2018, when GDPR came into force, it has affected all companies, institutions, and individuals across the European Union, as well as the companies outside of European Union territory that handle personal data of European's citizens. The main objective of GDPR is to protect digital rights of EU citizens.

The office for personal data protection (OPDP) has the main function in area of personal data protection in the Czech Republic. Since 2016, the OPDP is member of government working group that discuss problematics and impact of GDPR. On OPDP websites there is basic information about the changes that the Regulation introduce (3).

GDPR in the Czech Republic replaces the Act No. 101/2000 Coll., on protection of personal data, as amended. The rights and obligations in the current law on the protection of personal data will be replaced by the rights and obligations arising from the General Regulation. GDPR was accepted in April 2016. From then until May 2018, the companies and other users of personal data had time to investigate and analyse their current state of information systems and all procedures for the handling of personal data.

The partial objective of GDPR is to get rid of data that any data processing entity does not necessarily need. Another objective is to adjust consent to the processing of personal data. The consent must be obtained from any natural person when collecting such data.

GDPR orders to some data controllers or personal data processors to appoint an independent control person, called Data Protection Officer (DPO), who is responsible for the protection of personal data. The DPO oversees the compliance of the entities with GDPR, communicates with the Office for personal data protection, and perform internal activities such as audits and trainings.

Outside of personal data protection, General Data Protection Regulation also introduces new obligations for personal data processors, high sanctions for entities that are not compliant, and strengthens citizen's rights in terms of access rights and the deletion of personal data.

European directive 95/46/ES came into effect in 1995. At that time there were no cloud storages, no social networks, nor other technologies, therefore, the directive 95/46/ES was very outdated and there was a need for a new regulation. Personal data is a highly valuable commodity that can be used as a strategic asset; thus, personal data is an important part of our personal identity and therefore needs protection.

Nowadays, modern society is driven by processing of personal data, therefore, it is crucial to set up some rules of processing and movement of personal data. Sufficient protection of personal data during its processing is one of the main reasons of adoption of new legal framework which is represented by the General Data Protection Regulation.

2 Objectives and Methodology

2.1 Objectives

This thesis investigates impacts of General Data Protection Regulation, the new EU legislation. The main goal of the thesis is to analyse implementation of GDPR in selected organization. The thesis has three partial objectives. The first one is to study a current state and to make a literature review of the personal data protection framework in the European Union. The second one is to evaluate possible consequences of GDPR for selected organization and the last one is to propose an approach to GDPR compliant data management for the given company.

2.2 Methodology

The methodology of the thesis is based on analysis of implementation of General Data Protection Regulation rules. The practical part is focused on impacts of GDPR in a selected organization. The scientific methods such as analysis, synthesis, comparison, induction and deduction will be employed. By taking qualitative and quantitative approaches, a GDPR compliant data management approach will be proposed. Based on the theoretical part and outcomes of the practical part, final recommendations will be formulated.

3 Literature Review

General Data Protection Regulation is a substitution for directive 95/46/ES which is related to the Act No. 101/2000 Coll., on protection of personal data, as amended. The General Regulation itself is not a directive from European Union that each member country must implement. It is rather an EU regulation without possibility of major modification that is valid across all member countries.

3.1 GDPR background

In 24.10.1995, directive of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data, was introduced (1). In mid 90's there were no social networks, no cloud drives, nor a number of other technologies. Therefore, nowadays this directive is outdated.

Breach, fraud, or theft of personal data poses significant danger for citizens of the EU; therefore, cyber security is the main objective for future. Contemporary data analysis techniques are able to collect data and can predict consumer behaviour. All of these threats contribute to an effort to ensure basic data security. GDPR was created due to the rapid digitalization and cyber-activation of our world (2).

3.1.1 GDPR Timeline

After a two-year period after its adoption, GDPR has been fully enforced across all the European Union in May 2018. The Regulation had to pass several milestones in order to reach the point where it is today (12). Following table shows the most important milestones in the history of the Regulation.

October 1995	The Data Protection Directive (95/46/EC) was adopted
October 1998	The Data Protection Directive (95/46/EC) was enforced
January 2012	Initial proposal to update personal data protection regulation by the European Commission
March 2012	Article 29 Working Party releases opinion to data protection regulation

October 2013	European Commission's LIBE (Civil Liberties, Justice and Home Affairs) Committee promotes new rules
March 2014	European Parliament votes to support GDPR in its first reading
December 2015	Co-decision of the Council of the European Union and European Parliament approved its version in its first reading, known as the general approach, allowing the Regulation to pass into the final stage of legislation
April 2016	GDPR is adopted by the European Parliament and the Council of the European Union
May 2018	GDPR is enforced

Table 1 GPDR Timeline. Available at https://www.gdpreu.org/the-regulation/timeline/

3.1.2 Working Party 29 and European Data Protection Board

So called Working Party 29 (WP29) was established on the basis of a provision 95/46/ES, Article 29. Until GDPR came into effect, WP29 was a significant entity in the field of personal data protection. Working Party consist of representatives of the supervisory authorities of the European Union member states (more precisely one representative of the European Data Protection Supervisor and one representative of the supervisory authority of each member state).

The outcome of WP29 is represented in the form of standpoints, recommendations and opinions. The task of the Working Party 29 is, in particular, to ensure the uniform application of the General Regulation and to monitor its implementation (3).

As of 25 May 2018, the Article 29 Working Party ceased to exist and has been replaced by the European Data Protection Board (EDPB). EDPB is independent and has its own legal personality.

Tasks of the Board are described in the Article 70 of GDPR. The main task is to ensure consistent application of the General Regulation. That includes monitoring and ensuring the correct application of GDPR, advising the Commission on any issue that is related to protection of personal data within the Union, advising the Commission on the correct form and procedures of information exchange between processors, controllers and supervisory authority. Moreover, another partial task of the Board is to examine any question covering the application of GDPR. This examination is done on request of one of

its members, on its own initiative, or on request of the Commission. European Data Protection Board has to always use guidelines, best practise and recommendations to ensure consistent application of GDPR.

3.2 GDPR

The full title of GDPR is Regulation (EU) 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/ES (General Data Protection Regulation). The main responsible body for GDPR legislation in the Czech Republic is Ministry of the interior. The control function was given to the Office for personal data protection (4).

Among personal data that are covered by GDPR belong name, sex, age, date of birth, personal status, photographic record and IP address. Given the fact that GDPR also applies to natural persons doing business, there are also organizational data, like e-mail addresses, telephone numbers and enterprise IDs, which are ranked as personal data.

3.2.1 Obligations resulting from GDPR

The controller of personal data has to consider the nature, scope, context and purpose of processing of personal data and take into account the probable risks to the rights and freedoms of natural persons. Everything must be adapted to the security of personal data.

General Regulation introduces additional obligations for data controllers (5). Processing of personal data or security breach poses a high risk to the rights and freedoms of a natural person, and it is therefore appropriate to apply following obligations:

- Obligation to keep processing records,
- consultation with the supervisory authority,
- appointment of Data Protection Officer,
- obligation to assess the impact on the protection of personal data (Data Protection Impact Assessment),
- obligation to report violations of personal data security to the supervising authority.

These obligations apply only to certain type of controllers, controllers, and processors, depending on their personal data processing activities.

According to the Article 30 of GDPR, the basic instrument for every data controller are records of processing activities. These records contain general information on the processing that will enable the controller to make the processing easier to use. Data Protection Officer role is to ensure that the processing of personal data by some controllers is compliant with the Regulation. Records of processing activities represent a substitute for notification duty, which was repealed by GDPR. Processing records are only general records about data processing. It does not contain daily activity record with personal information.

Obligation to keep the processing records does not apply to companies with less than 250 employees, unless the processing activities represent risk for rights and freedom of personal data subjects, or unless it contains processing of special data categories or judgements in criminal matters.

Impact assessment on the protection of personal data is described in the Article 35. If it is likely that certain processing method, especially when using new technologies, will result in high risk to rights and freedoms of natural persons, the controller has to perform impact assessment of the intended personal data processing operation before the data processing. A single assessment may be sufficient for a set of similar processing operations that represent a same risk.

The impact assessment on the protection of personal data is primarily required in following cases:

- Systematic and extensive automated processing of personal data of natural persons,
- large-scale processing of special data categories or judgements in criminal matters,
- extensive systematic monitoring of publicly accessible areas.

A list of types of processing operations that are subject to an impact assessment requirement for the protection of personal data is set up by the supervisory authority.

3.2.2 Rights of the data subject

GDPR gives rights to the data subjects (6). The purpose is to find a balance between data controller and data subject. The Regulation introduces reinforced system of rights of

objects. Comparing to the Act on personal data protection, GDPR updated the current rights and added new rights, such as right to portability.

The exercise of the rights of the data subject is a highly protected interest for which GDPR imposes a higher possible sanction than the breach of less important duty. Therefore, it is essential that data controller ensures the proper exercise of the rights of the data subject.

In those cases, where Data Protection Officer was appointed, he is the main coordinator of ensuring compliance with GDPR. If the Officer was not appointed, it is recommended to designate a person who will be responsible for protection of personal data of data subjects (3).

The catalogue of the rights of the data subjects and corresponding duties of the data controller have been extended by below mentioned rights, in order to ensure transparency.

- Right to information about the processing of personal data,
- right of the data subject to access its personal data:
    - right to obtain confirmation from data controller about data processing,
    - right to obtain a copy of the processed personal data,
- right to repair,
- right to object,
- right to restriction of processing,
- right of erasure,
- right to data portability,
- right to refuse to be the subject of automated decision.

According to the Articles 15 – 22, the data controller has **an obligation to provide information** of the taken measures to data subject within one month without undue delay. In special cases, the deadline can be extended to two months, however, the data subject has to be informed and reasons have to be provided. Right to information about processing of personal data is a fundamental right that fulfils the principle of transparency. Data controller has an obligation to inform data subject about processing of his or her personal data, it is an immanent duty.

Information to be provided where personal data are collected from the data subject is described in the Article 13 of General Regulation. According to paragraph 1, the controller should provide the data subject with below mentioned information:

- contact details and identity of the controller and his / her representative (if applicable),
- contact details of the Data Protection Officer (if any designated),
- the purpose of the processing for which the personal data was collected and legal reasons for the processing,
- the recipient of category of recipients of the personal data (if any),
- any intention of the controller to transfer personal data to a third country.

Regarding the information provided in the case where personal data were not obtained from the data subject, data controller has an obligation to provide an information (within reasonable time after obtaining the personal data).

Data subject has **right to access** its personal data in order to check whether the personal data were processed or not. In case of data processing, data controller must provide purpose of data processing, recipients whom personal data have been or will be made available, information about personal data source, and the scheduled time for which personal data will be stored. Furthermore, the data subject has right to require modification or deleting of personal data.

As stated in Article 15, paragraph 1, the data controller has an obligation to provide confirmation to data subject whether his or her personal data are processed, how the data is processed and following information:

- the purpose of personal data processing,
- the categories of concerned data,
- the recipients or category of recipients to whom the personal data have been or will be disclosed, in particular recipients from the third countries or international organisations,
- the time period for how long the personal data will be stored. If the time period is not possible to determine, there is a requirement to state criteria used to determine that period,
- the existence of the right to request the data controller of rectification or erasure of personal data,

- the right to lodge any compliant to supervisory authority,
- any accessible information about source of personal data (if not directly collected from data subject),
- the existence of decision-making that is done on automated basis, including profiling.

Paragraph 3 in the Article 15 is describing that data controller is obliged to create a copy of the personal data undergoing processing. Copy and information should be provided free of charge. The controller may charge reasonable fee for other copy, the fee should not exceed administrative costs. In those cases where data subject request information by electronic means, the data controller should provide the information using electronic form. Since the copy of information can contain the personal data of other data subjects, the data subjects have the right to be informed of the appropriate safeguards.

Another essential right of the data subject is **right to repair**. In line with the principle of accuracy (which states that all personal data has to be correct and updated), there is a right of the data subject to request the data controller to repair any inaccurate personal data. Moreover, the data subject has the right to complete incomplete personal data. When the data controller receives this request, he has a duty to examine request from data subject and, if necessary, he has an obligation to perform requested changes.

The data subject has **right to restriction of processing** of his / her personal data. This measure is only temporary (as opposed to disposal of personal data). This right is described in the Article 18. General Regulation orders data controller to restrict the processing under following circumstances:

- the data subject denies the accuracy of the personal data (data controller must have some time to verify the accuracy of the data)
- processing is unlawful and the data subject rejects the deletion of personal data and instead requests that their use be restricted
- the controller no longer needs personal data for processing, but the data subject requires the personal data for purposes of identifying, exercising or defending legal claims
- the data subject has raised an objection to processing until it has been ascertained whether the legitimate reasons of the controller outweigh the legitimate reasons of the data subject

If right to restriction of processing was applied to personal data, they can be processed only with the consent of the data subject, or for the purpose of identifying, enforcing or defending legal claims or for protecting the rights of another natural or legal person.

Right of erasure represents the obligation of data controller to delete personal data in case when at least one of the following requirements is fulfilled:

- personal data is no longer required for purposes for which they were collected or processed,
- data subject opposes processing of its personal data and there are no legitimate reasons for the processing,
- data subject withdraws consent and there is no other legal reason for the processing,
- personal data was processed unlawfully,
- personal data must be deleted to meet legal obligations,
- personal data were gathered in connection with the provision of information company services.

In some cases, data controller has obligation to keep personal data, for example employee's data. In this case, data subject cannot request the removal of all personal information.

Above mentioned reasons do not apply when the processing of personal data is required for following reasons (Article 17, paragraph 3):

- for exercising the right of freedom of expression and information,
- for a compliance with a legal duty which requires by European Union or Member state law to which the controller is subject or for the performance of some task that data controller has to carry out in a public interest,
- for archiving purposes that are required by public interest, of for purposes of historical or statistical research
- for the defence or exercise of legal claims.

Data controller is responsible for the personal data for whole time until the data is fully erased or anonymised, which is another option for personal data disposal. Pseudonymised data cannot be considered as anonymised, therefore, this data has to be handled as personal data.

Right of data portability enables data subjects to request data controller to provide their personal data structured and machine-readable form. The data subject can provide these data to another controller. However, this action can be done only under certain conditions; when the processing is based on legal reasons, and when processing is done automatically. The exercise of the right of portability must not adversely affect the rights and freedoms of others.

The data subject has **right to object** in case the personal data are processed on the following legal grounds: when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or when processing is necessary for the purposes of the legitimate interests of the third party or the data controller.

In case that data controller does not have legitimate reason for processing of the data, which prevail over the interests or rights of the data subject, processing of data is no longer possible.

Right to refuse to be the subject of automated decision refers to option when the data subject will not be the subject of a decision that is based exclusively on automated processing. It cannot be decided about legal effects without human intervention. For example, a driver cannot receive fine for exceeding speed limit without examination from human. Automated decision is allowed in cases such as when a conclusion of the contract or the performance of the contract is necessary, or when automated decision has explicit consent of the data subject.

3.2.3 Sanctions

The Article 83 of the Regulation describes general conditions for imposing administrative fines (7). This is the responsibility of supervisory authority. Administrative fines have to be effective, proportionate, and dissuasive. The amount of the administrative fine is not given, it is imposed according to the circumstances of each individual case. Fines are not given for each violation of the Regulation, in some cases, the data controller can be warned that some processing of personal data are likely to violate GDPR. In other cases, the controller can receive admonition, or he may be ordered to comply with the data subject's request.

There are several general conditions for imposing administrative fees, as described in the Article 83, paragraph 2:

- the gravity, nature and duration of the infringement (taking into account the nature, extent or purpose of the processing),
- whether the infringement was committed intentionally or negligently,
- actions taken to mitigate the damage caused to data subjects,
- the degree of responsibility of the data controller or data processor (taking into account organisational and technical measures)
- all relevant prior violations caused by data controller or processor,
- the degree of cooperation with the supervisory authority in order to remedy the breach and mitigate its possible undesirable effects (whether the violation was reported by data controller to supervisory authority),
- the categories of personal data affected by the breach.

According to the severity of the violation that controller has committed, the amount of the fines is divided into two groups. A fine may be granted either to the amount:

- of 10 million EUR (or up to 2% of the total worldwide annual turnover in the case of an enterprise)
- of 20 million EUR (or up to 4% of the total worldwide annual turnover in the case of an enterprise)

A higher fine is granted to those, who significantly violate the Regulation. It depends on severity of the violation, nature, number of injured data subjects, if it was intentional or negligent violation, and the duration of violation. The data subject has the right for financial compensation in the event of material or immaterial damage.

3.2.4 Data controller, data processor

Data controller is defined in GDPR in the Article 4, paragraph 7 as: *"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"*

The main responsibility of the controller is to ensure that appropriate technical and organisational measures are in place. The measures are implemented for the reasons of demonstration that processing of personal data is performed in accordance to the General Regulation. Those measures must be reviewed und updated when necessary.

GDPR take into account the possibility of joint controllers. This is possible when the purpose and means of processing are jointly determined by two or more controllers who define their shares in the responsibility for the performance of the obligations. The respective responsibilities should be determined in a transparent manner, as described in the Article 26.

Definition of the data processor can be found in paragraph 8: *"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*

Processing of personal data by processor should be on the basis of contract or other legal act under European Union or Member State law. The contract or legal act set out the subject matter, the nature and purpose of the processing, the obligations and rights of the controller, the type of personal data and categories of data subjects, and duration of the processing. According to the Article 28, paragraph 3, the contract or other legal act must also guarantee certain circumstances of processing.

Any data controller can use data processor as a support for processing of personal data. This processor should use proper organisational and technical measures with regard to nature and category of personal data to ensure that the processing is in accordance with the Regulation. The processor does not release the controller from the responsibility for the processing of personal data.

There is also a possibility of joint processors, however, it is necessary for the data controller to give written permission to all data processors. The purpose of this permission is to ensure that the controller, who is primarily responsible for the processing, knows who process the personal data.

3.2.5 Data Protection Officer

Designation of Data Protection Officer (DPO) is described in the Article 37. Main task of DPO is to control whether the processing of personal data is in compliance with GDPR. Partial tasks include training of worker, internal audit, and the overall internal data

protection agenda. DPO has to perform all tasks in an independent manner. The Data Protection Officer should be appointed on the basis of professional qualities, in particular, professional knowledge of data protection rights and procedures. The General Regulation does not specify the precise requirements for the education of a DPO in terms of academic titles.

Data controller and data processor have to appoint DPO under following conditions:

- processing of personal data is performed by a public body or a public authority, with the exception of courts acting within their jurisdiction,
- the main activities of the data processor or controller consist of processing operations which, due to their nature, scope or purpose, require extensive regular and systematic monitoring of data subjects,
- the main activities consist in the extensive processing of specific categories of personal data and personal data relating to convictions in criminal matters.

The Regulation allows to appoint only one DPO for several companies, however, the Officer has to be easily accessible for every single company. Similarly, the organizational structure and size of public authority or a public body may be taken into account. Where appropriate, only one Data Protection Officer can be appointed.

DPO must have direct access to the management of the organization. In other words, the Officer should be directly subordinated to the senior management of the controller or processor in order to not have any intermediator when there is need of accessing personal data.

GDPR does not specify any requirements for certification of DPO, therefore, the Protection Officer does not have to have any certification and the controller or processor can appoint any person who has sufficient knowledge of personal data protection and GDPR.

The Officer is bound by secrecy in the performance of his duties and, in particular, is not personally liable for non-compliance with GDPR, because it must be the data processor or data controller who must ensure compliance.

3.2.6 Special categories of personal data

Some personal data are of such a nature that the data subject can be damaged at work, at school, in society, or may cause him / her to be discriminated. For these reasons,

there exist group of personal data (that are considered as highly sensitive) with increased protection during processing.

Sensitive personal data include personal data about racial or ethnic origin, religion, political orientation, philosophical beliefs, health condition, genetic and biometric data, and sexual orientation or life.

Special categories of personal data can be processed under following conditions:

- the data subject has provided an explicit consent,
- processing of personal data is necessary for the fulfilment of obligations in the field of labour law, social security and social protection,
- processing is necessary for protection of important data that belong to data subject or another natural person in case when data subject is not legally or physically qualified to consent,
- processing is necessary due to an important public interest,
- processing is necessary for the assessment of work ability of an employee, for preventive medicine or medical diagnostic, and for the purpose of providing health or social care,
- processing is necessary for the purposes of archiving in the public interest, for statistical purposes, and last but not least for scientific or historical research purposes.

The processing of photographs is not considered as processing of special categories of personal data. GDPR describes that processing of photographs is covered by the definition of biometric data only when the data are processed with special technical means that allows unique identification of a natural person.

3.2.7 Security of personal data

The data controller has to ensure a level of security by implementing appropriate technical and organizational measures. Implementation costs and state of the art, together with scope, context, nature and purposes of processing are taken into account. Therefore, every controller has to take adequate security measures to ensure, and to be able to demonstrate, that processing is carried out in accordance and compliance with the Regulation.

Among features of security of personal data belong, for example:

- pseudonymisation and encryption of personal data,
- data processor must ensure the ongoing confidentiality and integrity of processing systems,
- the systems must be available and resilient against hacking,
- in case of technical or physical incident, the restoration of availability and access to personal data must be possible in a timely manner,
- effectiveness of technical and organisational measures has to be regularly tested, assessed and evaluated in order to ensure the security of the processing.

As a breach of security of personal data is considered accidental or unlawful loss, destruction, alteration, unauthorized provision or disclosure of transmitted, stored or otherwise processed personal data. Data controller should consider whether the circumstances have to be reported to the supervisory authority or whether the data subject has to be notified in the event of a breach of security of personal data. These obligations arise in case when breach of security represents risk or high risk to the rights and freedoms of natural persons.

When data controller finds out a breach of security, he / she is obliged to report the breach to supervisory authority within 72 hours, as described in the Article 33. The obligation to report a security breach is only for the incidents with high severity in terms of rights and freedoms of individuals. Encryption and pseudonymisation can significantly reduce the risk of breach of security, therefore, using these methods can eliminate the necessity of reporting the breach to the supervisory authority.

Communication about the personal data breach to the data subject should be done without undue delay in case of a high risk to the rights and freedoms. Communication must be clear and plain language. In case of implementation of appropriate organisational and technical measures, the Controller is not required to communicate the security breach to the data subject.

A notification about security breach must describe the nature of the personal data breach, taken measures, possible consequences and, where applicable, contact details to the Data Protection Officer. A notification should also include the approximate number of data subjects and personal data records concerned. All personal data breaches should be

monitored by the Controller in order to enable supervisory authority to verify compliance with GDPR.

3.2.8 Data Protection Impact Assessment

The controller should carry out an assessment of the impact of processing operations that creates potential risk before the processing of personal data. Data protection impact assessment is required where a processing use new technologies and where nature, scope, purpose and context of the processing can result in a high risk to the freedoms and rights of individuals. Data Protection Officer should advice the controller when to carry out a data protection impact assessment. The assessment is, in particular, required in the following cases:

- a systematic and extensive processing of personal data is automated,
- processing on which decisions are based that creates legal effects concerning the natural persons,
- large scale data processing,
- processing of data that belong to special categories of data,
- processing of personal data related to criminal offences and convictions,
- monitoring of public areas.

According to GDPR, Article 35, paragraph 7, there are several parts that the assessment should contain:

- description of the processing operations and the purpose of the processing,
- an assessment of necessity of personal data processing operations,
- an assessment to investigate whether there is a high risk to the rights and freedoms of any data subject,
- security mechanisms and measures to demonstrate that the processing is in accordance with GDPR, and to ensure the protection of personal data

As described in the paragraph 8, all controllers and processors must take into account compliance with code of conduct during assessing of the privacy impact of any processing operations that are performed by such processor or controller. In case of a change of the risk constituted by processing operations, the controller should carry out a review to find out if processing is done in compliance with the data protection impact assessment.

3.2.9 Transmission of personal data to third countries

In contrast to the free movement of persons across the European Union, the free movement of personal data has several restrictions. The possibility to transmit data without any restrictions concerns institutional security. In other words, the same high standard of the legal framework for personal data protection in the European Union is applied and it is not necessary to subsequently ensure their institutional security. There has to be a legal ground in place every time when data processor transmits the personal data to another data processor. The obligation to have a legal ground also applies to cases where data is transferred outside the European Union.

It is not possible to transmit personal data to countries where there is insufficient legal protection of personal data, respectively, where the controller did not accept the tools to ensure this protection during handover. Transfer of personal data without any specific authorisation is possible in those cases where the Commission has decided that the other country or a territory has an adequate level of data protection.

There are several elements that must be taken into account when assessing the adequacy of the level of personal data and transmission protection:

- respect for basic rights and freedoms,
- the rule of law,
- compliance with legislation, both sectoral and general (including public and national security, defence and criminal law),
- implementation of such legislation,
- security measures (including rules for another transmission of personal data to another third country), professional and protection rules,
- judicial and administrative remedy for those data subject whose personal data are transmit,
- case-law (including enforceable data subject rights,
- existence of independent supervisory authority in the third country,
- international obligations and commitments of the third country.

According to the General Regulation, Article 45, there are several options for transmission of personal data to the third countries:

- transmission based on a decision on adequate protection,

- handover based on appropriate safeguards (binding business rules, standard contractual clauses)
- exceptions for specific situations where one of the two points above cannot be applied.

Development of the third countries should be monitored on an ongoing basis to ensure that protection of personal data is in accordance with GDPR. The list of the third countries that are no longer perceived as data safe should be published in the Official Journal of the European Union and on the Commission's website. Any decision that was adopted by the Commission should remain in force until amended, repealed or replaced.

3.2.10 Consent to the processing of personal data

The Article 4 of GDPR, paragraph 11, defines consent to the processing accordingly: *"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

Consent is always given for a particular purpose of processing that the data subject must know. Consent belongs to one of the several legal grounds on which the controller may process and process personal data if the processing cannot be subordinated to purposes for which consent is not required.

Data subject must have the freedom to decide whether to give consent or not. This consent is revocable, however, not always withdrawal of consent means the obligation of the controller to liquidate personal data, since the withdrawal of consent is for a particular purpose for which the personal data are processed, and the controller can process personal data for other purposes for which he uses a different legal reason for processing than the consent of the data subject. That means, once the consent is revoked, the Controller is obliged to cease the processing of personal data for the purposes defined in the agreement.

There is no obligation to have consent to the processing of personal data to every single processing. However, for those cases where processing is essential for the performance of the contract with the data subject or for the fulfilment of a legal obligation, there is a necessity to have a consent to the processing of personal data.

From a practical point of view, no consent can be enforced by methods such as restriction or failure to provide a service. The consent of the data subject is not required for the processing purposes that are necessary, for example, for the delivery of goods within an order in an e-shop or for the processing of personal data of employees for performance of a contract of employment or fulfilment of statutory obligations by the employer.

The General Regulation lays down the conditions for consent in the Article 7. According to paragraph 1, the controller should be able to prove that the data subject has consented to processing of her or his personal data. Moreover, consent must be distinguished from other facts to which the data subject expresses. Consent must be separated from the contract or business terms. The request must be written in plain language and in an intelligible and easily accessible form. Among rights of the data subject belong the right to withdraw the consent at any time and Data Controller should be ready to do so. This withdraw should be as easy as to give consent. Data Controller can in some cases process specific amount of personal data even without consent for processing, this is depending on the kind of service or product.

3.3 Principles of GDPR

GDPR lays down basic data protection principles which can be in other words described as an overview of the most important duties that data processor and data controller must follow when they want to process personal data in accordance with the Regulation. There are six data protection principles, described in the Article 5, and are as follows:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

3.3.1 Lawfulness, fairness and transparency

The first principle is discussing lawfulness, fairness and transparency. As it is set out in the Article 6, the **lawfulness** of processing is essential (8). The processing is illegal

when there is no lawful basis. According to the Article 6, processing is lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
- processing is required for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- processing is necessary for compliance with a legal obligation to which the controller is subject,
- processing is necessary in order to protect the vital interests of the data subject or of another natural person,
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority entrusted in the controller,
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Fairness refers to fair processing of personal data. In the other words, the processing must match the description. This principle requires that the controller (8):

- is open and honest about who he is,
- collects data from those who are legally authorised to provide the data,
- only processes the data in a way that the data subject could reasonably expect,
- does not use the data in a manner that could have an undue negative impact on it.

Data controller has to inform data subjects in a clear and understandable way how they use and process personal data in order to be in compliance with **transparency** principle. The principle of transparency also requires that any information relating to the processing of personal data is accessible without obstacles. Transparency principle is mostly used in provisions governing the rights of data subject, mostly information about collecting of personal data and right to access personal data. Moreover, transparency

principle can be observed in those cases where there is a personal data security breach, which represents a high risk to rights and freedoms of data subject.

3.3.2 Purpose limitation

According to this principle, personal data must be collected for explicit, specified and legitimate purposes and not further processed in a way that is incompatible with these purposes. Further processing for archiving purposes that are considered as interest of public, or purposes of historical and scientific research are not considered incompatible with the original purposes.

The purpose of the processing of personal data is important because it is based on the legal reason for the processing of personal data and other obligations (3). Article 6, paragraph 1(b) describes that processing is necessary for the performance of contract. If the purpose of processing is met, it is the responsibility of the controller to liquidate all personal data unless there is another legal reason for which personal data could be processed.

The only exception for further processing of personal data, where personal data can be processed beyond the original purpose is processing of personal data in the public interest, for scientific or historical research or processing for statistical purposes.

The General Regulation, Article 25, paragraph 2, describes that the controller should implement appropriate organisational and technical measures to ensure, that only personal data that are necessary for each specific purpose of the processing are processed.

3.3.3 Data minimisation

As described in the Article 5, paragraph 1(c), personal data must be relevant, adequate and there should be kept only those data that are necessary in relation to the purposes for which they are processed. Because of these above-mentioned reasons, data minimisation principle is closely related with the purpose limitation principle. Data minimisation principle prevents the data controller from requiring more data than is strictly necessary in relation to the legitimate purpose. Minimisation principle is a security element because if there is less data processed there is less risk of personal data breach.

As for the purpose limitation purpose, the principle of data minimisation is also linked with Article 25, paragraph 2 of GDPR which directs the data controller to implement appropriate organisational and technical measures to ensure, that only personal

data that are necessary for each specific purpose of the processing are processed. This obligation relates to the amount of personal data collected, the extent of processing, the availability and the storage period (3).

3.3.4 Accuracy

GDPR describes the accuracy principle as follows: personal data must be accurate and up to date (where necessary). Any inaccurate data shall be erased or rectified in a timely manner.

The controller is obliged to update personal data of the data subject if he receives a request from the data subject to do so. In those cases where personal data is apparently inaccurate, the controller has to accept reasonable measures in order to have inaccurate data updated or deleted. For example, data controller is entitled to update apparently inaccurate data like typing error in a given name, or error in a domain in an email address. Several e-shops require to type email address two times, this prevents the possibility of typing error to minimum. The same measures are used for typing a password.

Accuracy principle is predominantly connected with right to repair and right to limit the processing, according to which the data controller has to limit the processing of personal data in those cases when data subject does not agree with the accuracy of his personal data.

3.3.5 Storage limitation

This principle describes how the personal data should be kept. As stated in the Article 5, paragraph 1(e), all personal data are supposed to be kept in a form that permits identification of data subject. These data can be kept for no longer than is necessary for the purposes for data processing. In those cases, where personal data are stored for the purposes of public interest, historical or scientific research purposes, data can be stored for a longer period of time insofar as the personal data will be processed. Nevertheless, data must be processed in accordance to the Regulation in order to ensure rights and freedoms of the data subject.

The Article 17, paragraph 1(a) describes Right of erasure (‘right to be forgotten’). According to this Article of GDPR, the data subject has a right to have his or her personal data erased without undue delay, when there is no necessity of processing of personal data.

Data controller has an obligation to erase personal data if there is no necessity to store personal data, because the purpose of the processing was met and there is no more reason or purpose for processing of personal data.

One of the forms of erasure of personal data is data anonymization. Transfer of data to anonymous form is beneficial for data controller because there is possibility of using the anonymous personal data if the data is useful (3).

3.3.6 Integrity and confidentiality

As stated in GDPR, integrity and confidentiality principle discuss the need of using appropriate technical and organisational measures during the personal data processing. Moreover, the data shall be processed in a way that ensure appropriate security of personal data. Processing must include protection against unauthorised and unlawful data processing and there also must be protection against accidental destruction, damage or loss of personal data.

The requirement for proper security is described in the Article 32 and Article 25 of the General Regulation. Security of processing of personal data must always correspond to the nature, scope, context and purpose of the processing. The controller and the processor should implement appropriate organisational and technical measures to ensure low risk of security breach. Those measures involve pseudonymisation and encryption of personal data, ability to ensure ongoing confidentiality, reliability, integrity and availability of the processing system, and ability to restore access to personal data in a timely manner in cases of technical or physical incident.

3.4 Digital personal data

As stated in GDPR, provision 30, "*natural persons may be associated with online identifiers that are provided by their devices, tools, applications and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags*." This can leave traces that can be especially used when combined with unique identifiers and other information received by servers to create and identify individuals' profiles.

3.4.1 Cookies

Cookies are small files that are used by marketing companies to collect information about Internet users. These files are in a text form and are saved on a user's hard drive by a Web server. Cookies remember information about user and what are the user's preferences. They are designed to contain a modest amount of client-specific and website-specific data and are accessible either by a web server or by a client computer. Thanks to cookies, the relevant server remembers the default settings for the web page. Cookies make personalization easier. Original purpose of cookies was to assist e-shop users with their shopping; however, they have become a tool for the invasion of privacy (9).

GDPR sets out minimal requirements for communication with user. It must be clearly stated what is the subject of consent. The user should agree to use cookies and the method of give or not to give consent must be clear. According to the Regulation, consent to allow cookies could be given by using appropriate browser settings (where technically feasible and effective), in case that provided consent is not automatically set (2). However, GDPR does not regulate the ways how to obtain consent to the use of cookies.

Any advertisement network, as a third party that is using cookies, must comply with the Regulation and always ask for the consent to use the cookies on their Web pages. Supervisory authority must control whether those Web pages use a proper form of consent to use the cookie files. Unofficially, there are several recommendations:

- every consent from the user must be documented,
- consent can be obtain using a checkbox,
- implied consent can be obtained. In other words, user agree with the use of cookies when he/she continues with the use of a Web page. However, it has to be clearly stated.

There is no necessity to use consent for using the cookies for those cookie files that are necessary to provide the service requested by the user. To this group belong session cookies, authentication cookies, and cookies to help users.

3.4.2 IP addresses

The Regulation clearly states the responsibilities of data controller in case when a data subject requests an access, especially in the context of online services and online

identifiers. The controller should use all possible and reasonable measures to verify the identity of a data subject.

3.5 ISO 27001:2013

The ISO 27001:2013 standard (Information Security Management Systems) provides a framework for information security management best practice that helps organisations to achieve compliance with regulations such as the European Union General Data Protection Regulation. Additionally, this standard helps to protect client and employee information, manage risks to information security, protect information such as financial data and intellectual property, and protect the company's brand image.

ISO 27001 sets out the requirements of the Information Security Management System (ISMS), which is defined as 'a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives' (10).

The Information Security Management system mainly protects following key aspects of information:

- Confidentiality – the information is only disclosed or available to authorized people
- Availability – the information is usable and accessible by authorised users only
- Integrity – the information is accurate and complete, and protected from corruption

Unlike GDPR, ISO 27001 does not focus solely on the protection of personal data, but on all sensitive information, whether personal data, sensitive company data or, for example, partner organizations. On the other hand, GDPR sets out minimal requirements for the protection of personal data, like right to information, right to be forgotten, or transmission of personal data to third countries. ISO 27001 does not deal with these requirements.

ISO 27001 management will help with the implementation and comparison of GDPR requirements (11). Among the most important requirements belong encrypting, confidentiality, integrity and availability, risk analysis, business continuity, notification

duty, testing and evaluation. These requirements are more described in following paragraphs.

ISO 27001 recommends encryption as one of the measures that helps to eliminate identified risks. Implementation of controls in a given company is carried out on the basis of a risk assessment. Companies that follows ISO 27001 already identified and assigned the necessary measures, so they are more easily compliant with GDPR.

Another basic requirement of ISO 27001 is integrity, availability and confidentiality of information. These requirements help organizations to meet GDPR requirements regarding the right to information, right to repair or, if necessary, the right to be forgotten. With a functioning system, companies can more easily define who manages data, where data are stored, how they are handled, and can easily trace them.

ISO 27001 requires companies to carry out a risk analysis, including their evaluation, by identifying threats and system vulnerabilities. According to the results of the analysis, measures are subsequently put in place to maintain the confidentiality, integrity and availability of information. On the other hand, ISO 27001 warns against excessive security rules that can cripple the society in achieving goals.

Business continuity belong to another essential requirement. The standard lists controls that help companies make information available in the event of incidents and emergencies. Controls ensure the availability of information in case of threats and protect the key processes from the consequences of extraordinary events.

According to GDPR, organizations have an obligation to report a security incident within 72 hours of detection. ISO 27001 sets a notification obligation for security events in the system setting and focuses on reporting to relevant authorities. GDPR also sets a reporting obligation on data subjects when it comes to data with a high degree of risk to the rights and freedoms of entities.

Companies certified under ISO 27001 have an information security system evaluated by an independent accredited certification body, so they are confident that their system meets the conditions defined by the international standard. The system goes through regular checks and evaluations, so companies do not have to worry about outdated measures and settings.

3.6 ISO 31000:2018

The ISO 31000:2018 standard (Risk management) provides framework, process and principles for managing risk. This standard is useful for any organization regardless the size of company, sector or activity. The standard provides guidance for internal and external audit. Organizations that are using this standard can compare their risk management practices with an internationally recognized benchmark and provide reliable principles of effective management and corporate governance (13).

ISO 31000 can be used to help organisations to improve the identification of external factors like opportunities and threats, increase the likelihood of achieving objectives, and effectively use and allocate resources for risk treatment.

Risk management is used in strategic, program, project, and operational management and decision making. The risk management process varies depending on whether the risk is related to long-term, medium- or short-term objectives.

- **Low risks**
    - They are most often at the operational level, with emphasis on short-term goals. However, decisions about these risks often affect both medium and large risks.
- **Medium risks**
    - They mostly affect medium-term goals at the level of projects or programs. In terms of time or cost, they have lower impacts than large risks. Their importance is important, but not strategic.
- **High risks**
    - These are most often associated with strategic decisions. Their impact affects not only the current but, in particular, the future situation. This is precisely why strategic risks should be addressed continuously.

Risk rating is composed by evaluation of probability and impact of risk. Risk assessment matric can be created based on these determinants (15, 16).

Companies use the risk assessment matrix to measure the size of a risk and to determine whether they have appropriate controls or strategies to minimize the risk (18). Simply, the risk assessment process is composed of following processes:

1. **Identifying the risks**

- With regards to GDPR it is crucial to identify risks connected with protection of personal data.
- Risk has two basic components - vulnerability and threat. In the case of the processing of personal data, this is in particular:
  - Accidental destruction
  - Alteration
  - Unauthorised access to personal data
  - Unwanted modification of personal data
  - Loss of personal data
- Vulnerability is a term used to designate a weakness or lack of an asset. Vulnerability makes threats possible.
- Threat is a term used to denote the source of a negative event, power, person, or activity that wants or can damage an asset. The threat has an undesirable effect on safety or can cause damage, loss, undesirable change, or another undesirable phenomenon.
- Threats can be divided in following ways:
  - **Human factor** – it is essential to ensure proper organization measures in terms of assigning rights of access to personal data to employees and try to limit the necessity of these accesses to a minimum.
  - **Working environment** – insufficient work environment (low physical workplace safety) increases the risk of compromising personal data on the places where it is handled.
  - **Funds** – lack of funding can lead to a lack of technical security of personal data, or it may also have a negative impact on the skills and training of employees.
  - **Technical means** – the technical means of securing personal data are a basic measure of their protection. Apart from the physical security of paper documents, there has to be especially higher security of the IT infrastructure for storing electronic data in which personal data are stored.

        - **External suppliers** – the use of external suppliers is one of the main sources of potential breaches of personal data security rules and as such must be subject to sufficient formalization and control.

2. **Determination of risk criteria**
    - The numerical values with five levels of the probability and the impact of the risk are determined in the risk analysis process.
    - **Probability of risk** – takes into account many different aspects like:
        - given circumstances (storage of personal data with regard to the risk of physical damage)
        - business experience (number of similar incidents in the past)
        - general statistics (about data protection breaches)
    - The probability of each risk is divided into a numerical scale as follows:
        1. Excluded – a risk has never occurred and is not going to occur
        2. Negligible – there is a low possibility of risk
        3. Probable – it is likely that risk will occur
        4. Almost certain – it is highly probable that risk will occur under the current circumstances
        5. Certain – the risk is appearing frequently
    - **Impact of risk** – evaluating the risk severity with regards to seriousness of data protection breach:
        1. Negligible – no impact
        2. Low – impact is in a limited time period with low severity, not critical
        3. Medium – impact is in a limited time period with low severity
        4. High – impact is permanent and has low severity
        5. Critical – impact is permanent and has high severity
3. **Assessing the risk**
    - Quantitative analysis of the most important risks (as described in the section above)
        - Low risk

- Medium risk
- High risk

- The risk assessment is carried out in the framework of the initial analysis of information assets, mostly as part of the initial analysis of the preparedness for GDPR implementation.
- Based on the assessment of the probability and impact, each score is calculated by multiplying the probability and impact value. This resulting score is then used to decide on the risk classification based on the matrix shown in the table below.

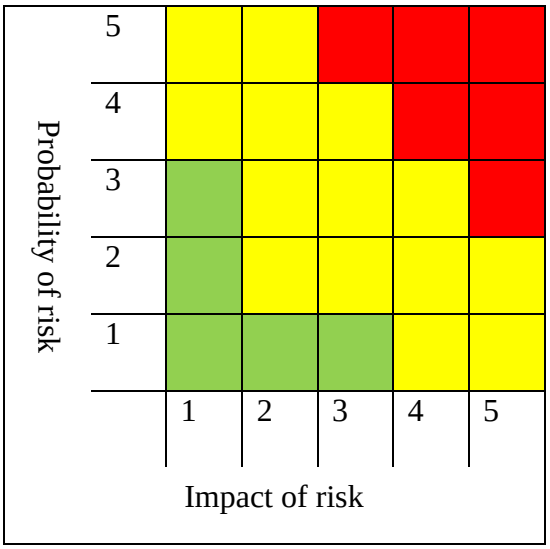

Table 2 Risk assessment matrix. Own work

Each risk will be assigned a classification based on its score as follows:

- High risk: 15-25
- Medium risk: 4-12
- Low risk: 1-3

4. Risk management

- The management of identified risks is related to the adoption of measures designed to reduce either the likelihood of risk activation or to reduce the negative impacts associated with risk activation. In both cases, it is a measure aimed at transferring risk from a high-risk zone to a medium or low risk zone or transferring a medium risk to low risk.

4 Practical Part

Practical part of this thesis investigates impacts of General Data Protection Regulation in a selected organisation. For the purposes of the thesis has been chosen a company engaged in programming, network administration, website development, and hardware and software sales.

An analysis of implementation of GDPR was conducted with the company's executive. A list of questions that should reveal the level of compliance with GDPR was presented. The results of the questionnaire will be further examined in the following chapters.

Data Protection Impact Assessment and Risk assessment is conduct in the other sections of the practical part. Even though these assessments are not required for all companies, yet it is preferable to conduct those assessment in order to comply with the Regulation in all aspects.

4.1 Analysis of the selected company

From publicly available sources can be found that the selected company was registered in the Business Register on September 8, 2017 as limited liability company. The company is a small business with one managing director and four full time employees. According to the Czech conditions for establishment of the limited liability company there must be a deposit in the amount of 200,000 CZK. The cash deposit was paid in full by the company's managing director. The business corporation was subject to the law as a whole in accordance with the procedure of § 777 (Article 5) of Act No. 90/2012 Coll., On Commercial Companies and Cooperatives. The company operates in the field of providing software, consultancy in the field of hardware and software, data processing, database services, network management, specialized software and hardware retailing.

In order to be compliant with GDPR, the company had to carry out several organisational and technological changes. By May 25, 2018 the company deleted all unnecessary server data, put the other data into fire safe, switched from http to https, all laptops and cell phones were encrypted, and made updated contract with each client (in the order of units to tens of new contracts). The majority of clients have signed the contract; however, one client had few comments to one contract provision which had to be modified on the basis of the comment.

4.1.1 Questionnaire measuring GDPR compliance level

Questionnaire, containing questions necessary for the analysis, was created in order to measure compliance of the company with GDPR. The company's managing director received following list with questions of a different nature.

- What kind of personal data do you store and process?
  - Email address
  - Phone number
  - Date of birth
  - Place of residence
  - Sex
  - IP address
  - Bank details
  - Cookies
- Do you process sensitive personal data?
  - Racial or ethnic origin
  - Political orientation
  - Religion
  - Philosophical beliefs
  - Trade unions membership
  - Health condition
  - Sexual orientation
- Do you obtain and process personal data under a contract?
- Do you obtain and process only those personal data that are necessary for fulfilment of the contract?
- Under what legal reason do you process personal data?
  - The data subject provided consent to the processing of personal data
  - Processing is necessary for the performance of contract
  - Processing is necessary to meet legal obligations
  - Processing is necessary for the purposes of the legitimate interests of data subject or of the third party

    - Processing is necessary for the performance of a task carried out in the public interest
- Did you dispose all personal data for which you do not have a legal reason for processing?
- Is the information that the data subject receives (or is entitled to) easily accessible (internet) and comprehensible?
- Are personal data collected for certain, expressly formulated legitimate purposes?
- Do you dispose the data when the purpose of processing is met?
- Are there adequate technical and organizational measures in place to ensure that only personal data that is necessary for each specific purpose of the processing is processed?
- Do you process personal data that is relevant and limited to the extent necessary in relation to the intended purpose of the processing?
- Are personal data processed in exact form and updated if necessary?
- Are personal data stored in a form that allows identification of the data subject?
- Do you perform conversion into anonymous form as a form of data liquidation?
- Are the processed personal data adequately secured (through appropriate technical and organizational measures) against unauthorized or unlawful processing and against accidental loss, destruction or damage?
- Do you encrypt e-mails? Attachments?
- Do you record personal data processing activities?
- Are you aware of the obligation to report any personal data security breach to the Supervisory Authority?
- Did you cooperate with Data Protection Officer?
- Did you perform Data Protection Impact Assessment?
- Do you use pseudonymization and encryption of personal data?
- Are the systems always available and resilient against hacking?
- In case of technical or physical incident, is the restoration of availability and access to personal data possible in a timely manner?

- Is the effectiveness of technical and organizational measures regularly tested and evaluated to ensure processing security?
- Do you perform automated processing of personal data?
- Do you carry out extensive processing of personal data?
- Do you transmit personal data to third countries?
- Do you follow ISO 27001:2013?

Since GDPR was introduced to protect personal data of European citizens, the first question was asked in order to find out, if the company falls under the scope of the Regulation. The respondent stated that they process client's e-mail address and phone number. Processing of contact details is essential to keep the contact with data subjects and inform them about business activities or (as required from GDPR) about changes in processing of their personal data.

The company also processes personal identification numbers of employees. Personal identification number is a unique identifier of every Czech citizen. The number identifies the birth date and sex of a citizen. In this case, processing of identification number is necessary to meet legal obligations, as it is required for example for taxation purposes. Place of residence data is processed for all employees as it represents another legal obligation. Addresses of clients are also processed; however, client is a legal person, therefore, this contact detail does not fall under GDPR scope.

As far as digital personal data, the company process bank details of the employees in order to provide them a salary. For some clients, certain bank details can only be detected indirectly from an incoming payment. IP addresses of clients are not actively collected. However, the respondent stated that IP addresses can be obtain as a part of the logs because certain mail servers log IP addresses themselves. Cookies are used only for Google Analytics. On company's websites there is no information for customers that the cookies are used. According to the Czech legislation, there is no requirement to have a consent to use the cookie files. The website itself does not remember who has logged in. Moreover, the website uses session data that sign off the user after inactive session.

The company does not have any legal reason for processing of sensitive data like racial or ethnic origin, political orientation, religion, philosophical beliefs or sexual

orientation. Nevertheless, one of the company's client is rehabilitation centre. Network administration services are provided to this centre; therefore, the company has access to health condition of centre's clients. Since the company (the processor) process the data on behalf the rehabilitation centre (the controller), there is no need od appointing DPO or performing DPIA because this obligation is required from the controllers.

'Do you obtain and process personal data under a contract.' is another question that was asked in order to analyse the current state of GDPR compliance of the company. The Regulation clearly states that all data can be processed only under a contract. Any contract identifies both involved parties. This identification is not possible without personal data. The company has a valid employment contracts with its employees and business contracts with its clients.

A business company may come across different data, including personal ones, and as a result of ignorance of legal regulations or stereotypes, it may commit a violation of the Regulation and process data which GDPR rules prohibit. Therefore, according to GDPR, companies may process only those data that are essential for operating of the company. Our company fulfils this condition as they process only those personal data that are necessary for fulfilment of the contract.

There always have to be at least one legal reason under which are personal data processed. Consent to the processing of personal data is one of the most common legal titles for processing personal data. This legal title is mainly used by the company for marketing activities to inform the existing customer base and gain new customers for its products. The company process most of the personal data under consent of processing personal data.

Processing for the purpose of performance of the contract - this situation involves the collection and processing of data in the context of ensuring the performance of the subject-matter of the contract, such as the agreement of two entities that one will lead customer database of second entity. The respondent stated that the company does back up activities for rehabilitation centre, therefore, they have access to health condition of clients of the centre. These backup activities are done for the purpose of performance of the contract.

Processing to comply with legal obligations is a situation in which the law of the State requires that the entity provide some of the personal data of other persons in order to accurately identify and easily verify the data by a public authority body or by a person

exercising the public authority. Collecting data of the descendants of individual employees is required for the purposes of the Income Tax Act, therefore, the company fulfills the legal obligation to collect personal data.

The company does not process personal data on the basis that processing is necessary for the purposes of the legitimate interests of data subject or of the third party, nor for the reason that the processing is necessary for the performance of a task carried out in the public interest.

Disposal of personal data where processing does not have any legal reason belongs to essential principle of GDPR. Data controller has an obligation to erase personal data if there is no necessity to store personal data, because the purpose of the processing was met and there is no more reason or purpose for processing of personal data. The respondent stated that the data of clients of former employees were moved to encrypted external drives and inserted into a vault to which only two company managers have access. Because of legal reasons, the company has to store invoices for ten years. As it is stated in all contracts, in those cases when the company cease to work as a network administrator, all client's personal data and backups must be deleted. Erasure of personal data has never been done because the company has regular customers. However, data is erased when a customer does not cooperate. conversion into anonymous form as a form of data liquidation. One of the other options as a form of data liquidation is a conversion into anonymous form. However, given the fact that the company is a small business, no such anonymisation is done.

The Regulation clearly states that there must be adequate technical and organizational measures in place to ensure that only personal data that is necessary for each specific purpose of the processing is processed. Due to the fact that the company has only five employees, no guidelines or directives are implemented.

Given the fact that the company does not want to store and process unnecessary data, they handle only those data that is relevant and limited to the extent necessary in relation to the intended purpose of the processing. Clint's data is also processed in exact form and updated when needed. It follows that the company is in compliance with accuracy principle as the controller updates personal data of the data subject if he receives a request from the data subject to do so.

Identification of data subject is crucial attribute of storing of personal data. All personal data of employees are stored in a folder on One Drive. This folder is accessible only by the managing director of the company. Given the number of employees, there is no special identification, like personal ID, to distinguish between employees. Accounting data are stored in electronical form. Those data are accessible only for selected employees. Regarding the rehabilitation center, all data are stored in database at webserver. The company, as a webmaster, has access to the database through the encrypted https connection. Backup data from rehabilitation center are stored in encrypted computers.

The company has implemented appropriate technical and organizational measures to secure the personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage. All backups are stored in fire safe which provides protection against data corruption or theft. Furthermore, all company laptops and cell phones are encrypted with BitLocker. This full disk encryption feature is designed to protect data by providing encryption for entire volumes. Regarding intranet sites, all are secured by Hyper Text Transfer Protocol Secure, which has advantages in: authentication, confidentiality of transmitted data, and integrity of content. the effectiveness of technical and organizational measures is not regularly tested nor evaluated in order to ensure processing security.

Encryption of the email can help any company to comply with privacy laws, limit the risk of data breaches and hacks, and improve business security strategy. Even though that encryption is one of the data protection security measures specifically recommended in the Regulation, GDPR does not states that it is required. The company does not encrypt email, neither any attachments. However, all other data is encrypted in order to mitigate the risk of personal data breach. Pseudonymization is not used.

Article 30 of GDPR defines obligation to record processing activities. The controller shall maintain activities under its responsibility which should contain for example the purpose of the processing, name and contact details of the controller, and description of the categories of data subject. Nevertheless, these obligations are only valid to a company employing fewer than 250 employees unless the processing is likely to result in a risk to the rights and freedoms of data subject, or the processing includes special categories of data or personal data about criminal matters and offences. The company’s representative stated that there are no records of personal data processing activities.

Obligation to report violations of personal data security to the supervising authority belongs to elementary duty of data controller. The responsible person shall without undue delay, and no later than 3 days after becoming aware of it, contact supervisory authority about the data breach. The company is aware of this obligation.

Among other obligations resulting from GDPR goes an appointment of Data Protection Officer and obligation to assess the Data Protection Impact Assessment. DPO must be appointed where the main activities of the data processor or controller consist of processing operations which, due to their nature, scope or purpose, require extensive regular and systematic monitoring of data subjects, and where the main activities consist in the extensive processing of specific categories of personal data and personal data relating to convictions in criminal matters. Similarly, the DPIA is required in cases, such as automated systematic and extensive processing of personal data, or large-scale processing. The respondent stated that the company did not appoint Data Protection Officer, nor assessed Data Protection Impact Assessment.

The company implemented technological measures in order to ensure that all systems are always available. Intranet runs on webserver; therefore, availability is guaranteed. There were no penetration tests performed, so the resistance of the system against hacking is not confirmed. Though, the company uses commonly available systems that are continually updated.

Personal data must be appropriately secured at all times. Therefore, in case of technical or physical incident, the restoration of availability and access to personal data has to be possible in a timely manner. The company has backups of all data; however, it would take some time to restore the data in case of some incident with the primary storage. In case of software defect (for example database defect), it would take hours to restore the data. In case of hardware defect (burnout, flooding), all data would be restored in the order of hours or days.

GDPR forbids automated systematic and extensive processing of personal data because it cannot be decided about legal effects without human intervention. The only processing which is automated is when the client makes an order, an automatically generated invoice email arrives. Nevertheless, this processing is not considered as large scope processing of personal data.

The company does not transmit personal data to third countries. However, all files are kept on cloud storage whose server if physically located abroad. General principles for transfers are described in the Article 44. According to this article, only personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation subject to the provision of the Regulation. Hence, there is no restriction on storage of personal data on a cloud whose server is located abroad.

International standards ISO 27001:2013 and ISO 31000:2018 provide framework for information security management best practice and for managing risks. When companies follow these standards, it helps them with achieving compliance with the Regulation. Generally, small companies do not follow ISO standards and the company which this thesis is assessing is one of them.

4.1.2 Evaluation of the analysis

Based on the analysis that was performed in the previous chapter can be stated that the company is GDPR compliant. Thus, there is no requirement to appoint Data Protection Officer nor obligation to perform DPIA. Nevertheless, for the purposes of this thesis the impact assessment will be conduct.

4.2 Data Protection Impact Assessment

DPIA provides a view on the security of data processing, on the rights and freedoms of natural person and a compliance point of view. Data Protection Impact Assessment is a risk management tool for the data subjects' rights. The controller shall, prior to the processing, carry out an assessment of the impact of the processing operations on the protection of personal data. This assessment should be done in particular when a processing is likely to result in a high risk to the rights and freedoms of natural persons.

The form of the company together with description of the steps of processing must be determined at the beginning of the process. The company is limited liability company focused on management of computer networks and computers itself, website programming, and design and programming of intranet systems.

The company programming an intuitive administration website (Content Management System) that has been developing for over 10 years. Pages are programmed

in PHP with use of the Nette framework (self-usable components for PHP). Thanks to this feature the websites are modern and safe.

When using html encoding, the Bootstrap framework (an open source toolkit for developing with HTML, CSS, and JS) is used in order to have sites that are responsive and viewable on mobile devices.

The company does not make graphic designs, but they work with several designers to give the site a unique look. Or the customer can choose from dozens of finished templates.

For more than 10 years, the company has been developing intranet systems such as billing systems, CRM systems, order management systems, business case databases, theatre management, and booking systems. Typically, the intranet also includes print outputs to PDF and assembly generators.

Regarding network management, the company manages complete corporate computer networks - file server, mail server, application servers (such as remote desktop, database servers, accounting systems), active and passive network elements (routers, switches, Wi-Fi), printers, scanners and, of course, individual computers. Employees understand computers with Windows, Apple MacOS and Linux.

Another ability is to make complete design and build a network, or to take over an existing network and optimize it. The company takes advantage of remote administration, software is managed centrally and remotely. Servers use Hyper-V or VMware virtualization.

According to GDPR, data controllers are eligible to determine the precise structure and form of DPIA. Content of the assessment is described in the Article 35, paragraph 7. The assessment shall contain:

- description of the processing operations and the purposes of the processing,
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes,
- an assessment of the risks to the rights and freedoms of data subject, and
- the measures that are planned to be taken in order to address existing risks (security measures, safeguards, and mechanisms to ensure the protection of personal data, demonstration of the compliance with the Regulation)

4.2.1 Description of processing activities

Each processing activity starts with collection of personal data and ends with data disposal. In the table below are named the business processes with the description in order to understand the processing activities.

Business process	Description	Relevant information system	Supporting factors
Collection of personal data	Collection of client's personal data on the basis of a business contract Collection of employee's data on the basis of an employment contract	HW: Laptops and desktop PCs, fileserver, application server SW: Rehabilitation centre – tailored SW (app produced by the company), Medical software Amicus	Accountants, IT managers, employees, supervisors
Processing of personal data	All data is processed automatically, necessary documents are printed out in accounting department	HW: Laptops and desktop PCs, fileserver, application server SW: Rehabilitation centre – tailored SW (app produced by the company), *example of application layout on the screenshot below this table	Accountants, IT managers, supervisors, employees
Transfer of personal data	Transfer of invoices and contracts	HW: Laptops and desktop PCs, fileserver, application server SW: e-mail	Accountants, IT managers, supervisors
Storage of personal data	Invoices are kept as hardcopies in an archive room for 10 years Contracts are stored	HW: Laptops and desktop PCs, fileserver, application server, backup tapes	IT managers, employees, supervisors

	in Microsoft SharePoint. Backup tapes are stored in a fire safe.	SW: Office 365	
Elimination of personal data	Data storage media are destroyed at the end of retention period or at the end of the contract	HW: Laptops and desktop PCs, fileserver, application server, backup tapes	IT managers, supervisors

Table 3 Description of processing activities. Own work, based on https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

The company produced tailored software for the rehabilitation centre. One of the features of the application is reservation maker. As it can be seen on the figure below, the reservation include time and date, name of the rehabilitation centre employee who will be responsible for the operation, what kind of operational procedure will the patient take and, of course, the personal data of the employee – name and surname, telephone number, personal identification number, health insurance company, diagnosis, notes and an amount to be paid.

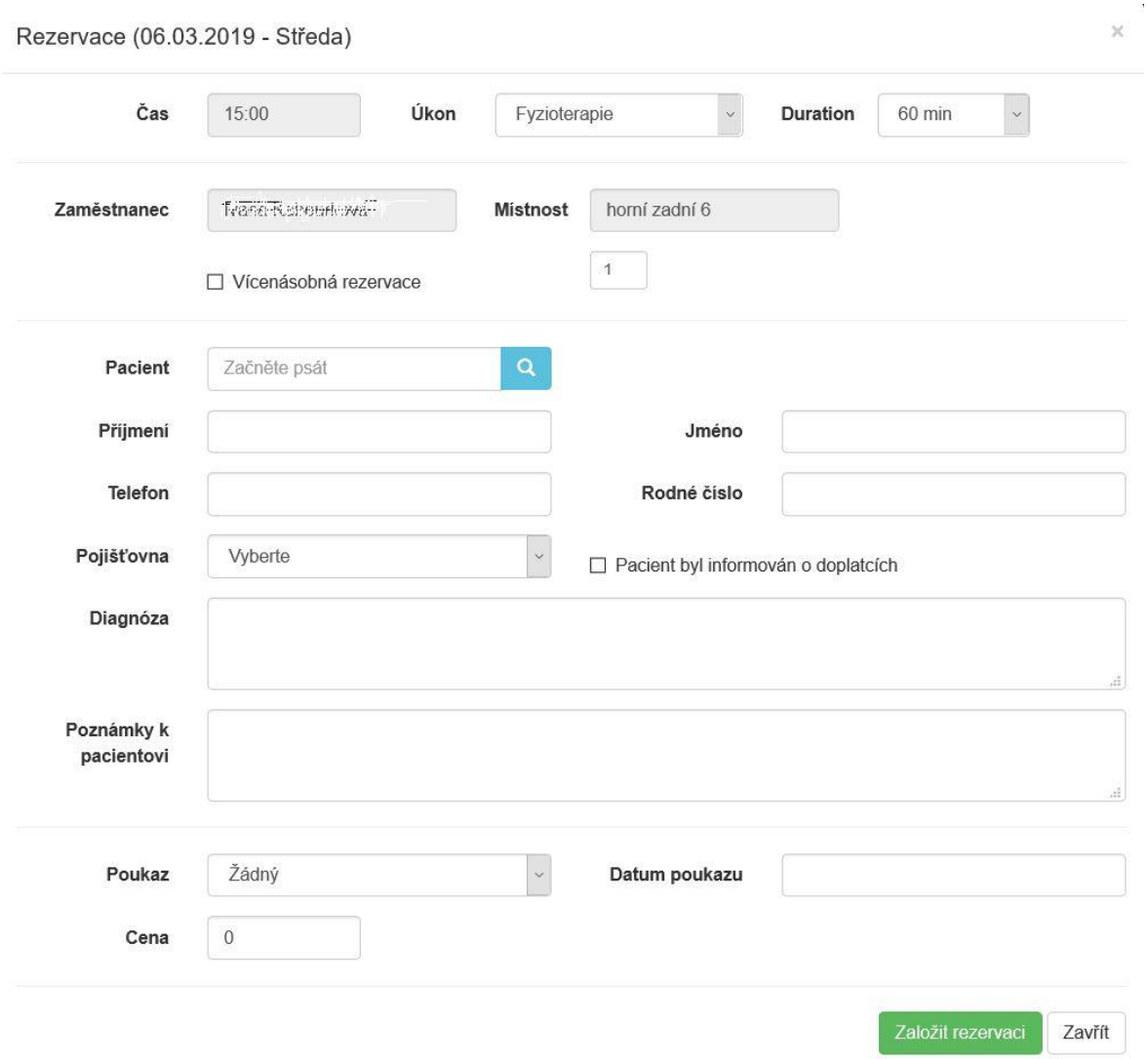

Figure 1 Rehabilitation centre reservation window

Description of processing activities has just informative character, therefore, no valuation from this assessment can be provided.

4.2.2 Assessment of the necessity and adequacy of the data processing activities

The company has two legal reasons to process the personal data. The first one is to comply with legal obligations. The law of the State requires that the entity provide some of the personal data of other persons in order to accurately identify and easily verify the data by a public authority body or by a person exercising the public authority.

Another legal reason is processing for the purpose of performance of the contract - this situation involves the collection and processing of data in the context of ensuring the performance of the subject-matter of the contract. These contracts involve employment and

business contracts. All processing of personal data is done only within the limits of the contract.

4.2.3 Assessment of risks for the rights and freedoms of the data subject

The Article 5 of GDPR sets out basic data protection principles which are essential with regards to protection of rights and freedoms of the data subject.

Data protection principle	Data protection risk	Status of the company – compliance view
Lawfulness, fairness and transparency	Article 5, 1. (a)	All data are processed lawfully, fairly and in a transparent manner. • The data subject has given a consent to the processing of his or her personal data for a specific purpose – Article 6, 1. (a) • Processing is necessary for the performance of a contract – Article 6, 1. (b)
Purpose limitation	Article 5, 1. (b)	Data are collected only for specified, explicit and legitimate purposes. Data are not further processed in a manner. that is incompatible with those purposes • Personal data of employees are collected on the basis of Labour Code – Article 6, 1. (c) • Personal data of clients are collected on the basis contract and are processed only to the extent specified in the contract– Article 6, 1. (b)
Data minimisation	Article 5, 1. (c)	The company does not store any personal data that are inadequate, irrelevant. Personal data are limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Article 5, 1. (d)	Only accurate data are processed. If possible, all data are kept up to date. Inaccurate data are erased without undue delay.
Storage limitation	Article 5, 1. (e)	Personal data are kept in a form which allows identification of data subject. Data are stored no longer that it is necessary – personal data are deleted at the end of the contract.
Integrity and confidentiality	Article 5, 1. (f)	Processing of personal data ensures appropriate security of data. Technical and organisational measures in order to protect data against unauthorised or unlawful processing and accidental loss, destruction or

		damage, are in place. Hardware like laptops and cell phones are encrypted with Bitlocker. Backups are stored in a fire safe.
Accountability	Article 5, 2.	The controller of the company demonstrates the compliance with Article 5, paragraph 1. The data protection measures are upheld by the controller. Data protection responsibilities are determined by the controller.

Table 4 Assessment of risks to the rights and freedoms of the data subject. Own work, based on https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

According to the assessment of risks to the rights and freedoms of the data subject, the data protection principles of the compliance view are fulfilled. Taking into account the described measures, the risk analysis in the area of data protection does not pose a high risk to the rights and freedoms of data subjects.

4.2.4 The measures planned to address risks

The controller's obligation is to describe what measures will be used in order to avoid violations of data protection principles. The Article 35, paragraph 7 (d) requires the determination of measures that ensure the protection of personal data and that prove the compliance with the GDPR requirements. The measures include safeguards, security measures and processes. The rights of data subject and other concerned subjects have to be taken under consideration.

4.3 Risk assessment

The main principle of GDPR implementation is the risk-based approach (both from the point of view of the data subject and from the point of view of the data controller and data processor). So, in the first step there is a requirement to assess the risks, then risks have to be evaluated. In the end, it is necessary to decide on the adoption of measures to reduce and eliminate the risk or to accept the risk.

There are a number of definitions for risk. The risk is most often defined as the product of the magnitude of the consequences of the undesirable event and the likelihood that the undesirable event occurs.

Risk analysis can be also processed in relation to the fundamental rights and freedoms of the data subject, such as:

- identity protection,

- the right to information,
- the right to protection of personal data,
- the right to mental and physical integrity,
- the right to privacy.

4.3.1 Identifying the risk

Five essential risks have been identified for the purpose of this thesis. Following risks represent possible dangers of processing of personal data.

- Accidental destruction
- Alteration
- Unauthorised access to personal data
- Unwanted modification of personal data
- Loss of personal data

Given the fact, that human factor can cause errors, there is low possibility that handling with personal data can bring about accidental destruction, unwanted modification of personal data and loss of personal data. Alteration or unauthorised access to personal data is unlikely to occur because the company has sufficient organisational and technical measures. Mentioned vulnerabilities are summarised in the following table.

Risk	**Vulnerability**
Accidental destruction	Possible
Alteration	Not likely
Unauthorised access to personal data	Not likely
Unwanted modification of personal data	Possible
Loss of personal data	Possible

Table 5 Vulnerabilities. Own work

One of the parts of risk assessment is also examining potential threats associated with vulnerabilities. Threats are cause by several factors, among which are mainly human factor, working environment, funds, technical means and external suppliers. There is a low probability of these threats because the company has implemented adequate organisational structure, therefore, division of roles is in place. Working environment is sufficient.

Nobody can enter the premises without access key, all data is stored on encrypted drives and backups are kept in fire safe. With regards to funding, it can be stated that it is sufficient. The company does not suffer of inadequate finance. Sufficient IT infrastructure is in place. Software is updated on regular basis. The company has several contracts with external suppliers. All contracts clearly stipulate roles, competences, tasks and responsibilities of the suppliers.

Threat				
Human factor	**Working environment**	**Funds**	**Technical means**	**External suppliers**
Organisational structure (division of roles) in place	Sufficient working environment, area is secured – can be accessed only by employees, backups in fire safe	Sufficient funding	Sufficient IT infrastructure, software is updated on regular basis	Contracts clearly specify roles, tasks, competences and responsibilities of external suppliers

Table 6 Threats. Own work, based on https://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr_14864_3805_11.html

In summary, there are no significant risks when processing of personal data. The risk is also limited due to the fact that the company is small business with few employees. Measures to prevent violation of basic principles, like integrity, confidentiality and availability were assessed in DPIA. These data protection objectives were considered.

4.3.2 Determination of risk criteria

In the second step of risk assessment, risk criteria have to be determined based on the numerical values with five levels of the probability and the impact of the risk. As stated in the theoretical part of this theses, those levels are:

Probability

1. Excluded
2. Negligible
3. Probable
4. Almost certain
5. Certain

Impact

1. Negligible
2. Low
3. Medium
4. High
5. Critical

The risks that are assessed in this thesis are mainly caused by human failure. The risks source is, in particular, employees, supervisors and IT managers who are responsible for processing of personal data. On the other hand, the risk can be caused even by natural disaster, like fire or flood. Given the fact that the company headquarter is not near a river, and backups are stored in fire safe, there is very low probability of this kind of risk. Another source of risk can be malicious code or attack from hackers. Even though the company uses recent versions of antivirus protection there is a probability that some malicious code might influence the processing. No penetration tests are done, so the company cannot assess the level of protection against hacker attacks. However, there is quite low probability of a hacker attack given the size of company and volume of clients.

In case of risk occurring, there might be negative impact on the company. The most critical impact is credibility problems of the company. The occurrence of this risk will result in decreasing of competitiveness on the market. Further impact, like disclosure of payment details of clients and employees can be cause by unauthorised access to personal data. This risk will also result in loss of clients.

Risk	Risk source	Probability	Impact
Accidental destruction	Employees, supervisors, IT managers	**2**	**2** - Credibility issues of the company
Alteration	Employees, supervisors, IT managers, hackers	**2**	**1** - Restoration of backups
Unauthorised access to personal data	Employees, supervisors, IT managers, hackers	**3**	**4** - Disclosure of bank details of clients and employees, loss of clients
Unwanted modification of personal data	Employees, supervisors, IT managers	**3**	**2** - Credibility issues of the company

Loss of personal data	Employees, supervisors, IT managers, malicious virus or code, flood, fire	**2**	**3** - Credibility issues of the company, decreased competitiveness

Table 7 Probability and impact of the risks. Own work, based on https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

4.3.3 Assessing the risk

Based on the assessment of the probability and impact, each score is calculated by multiplying the probability and impact value. This resulting score is then used to decide on the risk classification based on the matrix shown in the figure below.

Risk	**Score**
Accidental destruction	2 x 2 = **4**
Alteration	2 x 1 = **2**
Unauthorised access to personal data	3 x 4 = **12**
Unwanted modification of personal data	3 x 2 = **6**
Loss of personal data	2 x 3 = **6**

Table 8 Risk assessment. Own work

Four of five risks lay in a yellow zone which represents medium risk classification. Only alteration is classified as low risk. The classification of personal data into risk classes might have effect on further use of this data. In case of a risk occurring in a red zone (high risk), the data controller has to check whether a DPIA needs to be carried out. Moreover, in case of violation of personal data that belongs to high risk category, competent supervisory authority and the data subject has to be notified about this violation. Where the personal data belonging to the medium risk category are infringed, only the supervisory authority must be informed. The company does not face any high risk.

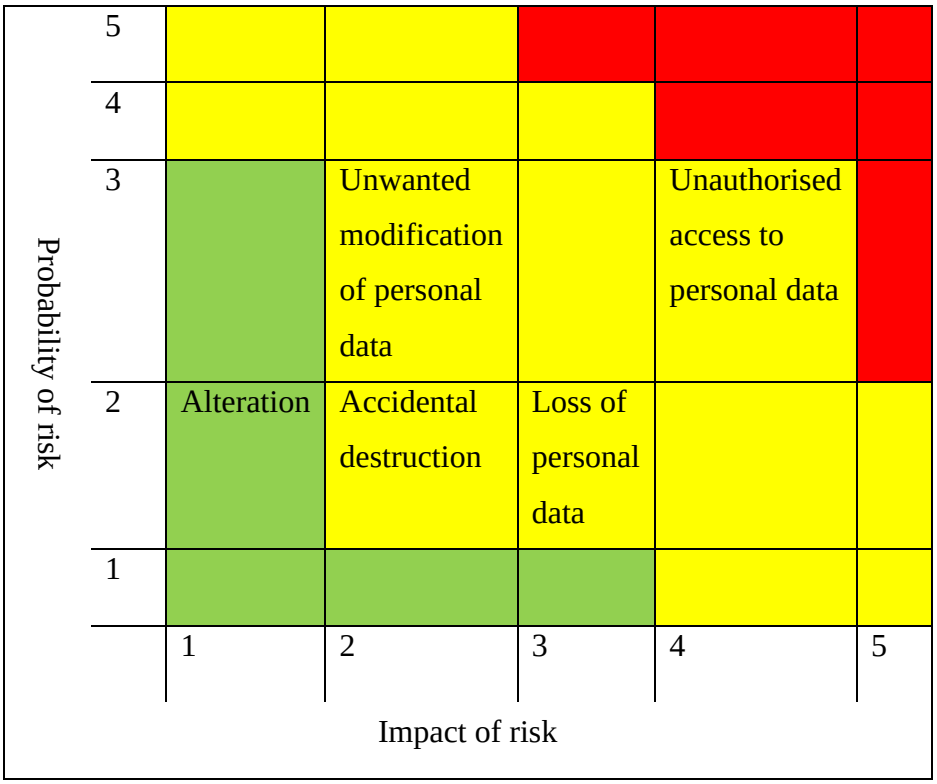

Figure 2 Risk assessment matrix. Own work

4.3.4 Risk management

One option to deal with risk is that the company has to adopt measures that will transfer risks from medium risk zone to low risk zone. Another way of dealing with risk can be risk avoidance where some categories of personal data will not be processed anymore. Some risks might also be accepted.

Security of processing, described in the Article 32, defines technical and organisational measures that shall be accepted by the controller and the data processor in order to reduce a risk and ensure a certain level of security. Among these measures belong:

- the pseudonymisation of personal data and its encryption,
- the ability to ensure ongoing confidentiality, availability, resilience and integrity of processing systems,
- the ability to restore access to personal data in a timely manner in case of physical or technical damage of the data,
- a procedure for regular testing, assessing and evaluating the effectiveness of organisational and technical measures in order to ensure the security of processing.

Although the company does not perform pseudonymisation of personal data, yet all data is encrypted. Due to the size of the company and the severity of the risks, accepted technological measures can be considered as sufficient.

An ongoing confidentiality, integrity, availability and resilience is ensured by regular updating of processing systems. Always the recent version of antivirus program is used. As far as the ability to restore access to personal data, there are backups to all data. Thus, in the event of physical or technical incident, the company is able to restore data in a timely manner.

Even though there is no procedure for regular testing, assessing and evaluating the effectiveness of organisational and technical measures in order to ensure the security of processing, due to the number of employees and size of the company it is not crucial aspect of security measures.

5 Results and Discussion

Practical part of this thesis analysed implementation of GDPR in the selected company. Qualitative and quantitative methods were used for creation of Data Protection Impact Assessment and risk assessment. On the other hand, the Results and Discussion chapter describes the costs connected with the GDPR implementation and discuss the satisfaction with the Regulation. Implementation costs data are used from price lists of the Czech providers of GDPR implementation.

5.1 GDPR implementation costs

There are several factors that influence the overall GDPR implementation cost. Among the basic factors belong size of the company, number of employees, number of clients and type and volume of personal data that the company handles. Between secondary factors belong, for example, training cost of the employee, customer GDPR privacy notification, and description of processing activities (18).

In case that an organisation does not process the personal data of EU citizens, the GDPR does not apply to them. However, in the World of current information technologies, it is recommended to have data privacy security measures in place. If an organisation processes personal data of EU citizens, following factors should be considered:

- Is an organisation data controller or data processor? Data processors are usually third parties which do not have to meet all GDPR requirements. On the other hand, data controller is fully responsible for all processing activities.
- In case of data protection risks, additional control measures should be implemented.
- An organisation should describe the category of personal data that handles.
- Monitoring of vendor compliance in case of existence of other organisations and third parties that process the same personal data.
- Data retention – data should be kept only for the least amount of time needed.
- Transferring of personal data to third countries.
- Additional requirements will apply in case of processing children's personal data.
- Testing of security controls that were implemented to secure personal data.

- Appointment of DPO.

Depending on the factors mentioned above, the roadmap to GDPR compliance will include some or all of the steps below. The real cost to comply will depend on how and at what scale is each step completed.

Assigning a Data Protection Officer

DPO has to be appointed by data controller only in those cases where processing of personal data is performed by a public body or a public authority, with the exception of courts acting within their jurisdiction; when the main activities of the data processor or controller consist of processing operations which, due to their nature, scope or purpose, require extensive regular and systematic monitoring of data subjects; and when the main activities consist in the extensive processing of specific categories of personal data and personal data relating to convictions in criminal matters.

The data protection officer without a legal background would cost around 100-200 EUR per hour. If the data protection officer is a lawyer, then they would cost around 300-500 EUR per hour. DPO can be individual person within a company or third-party provider. Even in those cases where DPO is not required, it is better to have someone to oversees GDPR compliance.

Recording of processing activities

According to the Article 30 of GDPR, the basic instrument for every data controller are records of processing activities. These records contain general information on the processing that will enable the controller to make the processing easier to use. The purpose of the processing has to be identified as well as any transfer of personal data to third countries.

The cost of recording processing activities depends on the volume of processed data and the number of employees in a company. Influencing factor is also the number of processes and number of data types.

Gap assessment

Even though the gap assessment is not obligatory, it provides important comparison between current controls, policies and procedures vs GDPR control requirements. Gap

assessment is done according to the ISO 27001:2013 standard (Information Security Management Systems) that provides a framework for information security management best practice that helps organisations to achieve compliance with GDPR.

The cost for a typical ISO 27001 assessment starts at 15,000 USD. Managing the cost of the ISO 27001 assessment is of course very important – and a sound approach, with experienced assessors will provide long-term value to the organization.

Policies and procedures

This step usually requires involvement of all employees who are responsible for processing activities. New ongoing policies and procedures have to be implemented and regularly updated in order to address GDPR data protection requirements. The cost of this step depends again on the volume of processed personal data and the number of employees.

Training of employees

Failure of human factor is one of the most common personal data security breaches. The money invested to GDPR compliance can go wasteless if the proper training of employees will not take place. Training of employees can be conduct by Data Protection Officer or by any other third-party provider with relevant skills and knowledge. The cost of training depends on the number of employees and on the training provider.

Compliance monitoring

Monitoring of compliance belongs generally to the most expensive step of GDPR implementation. This is an ongoing process which requires internal monitoring of compliance oversight responsibilities, which involves many departments, like IT and Operations, Sales, Marketing, and Development. This step requires significant investing in the security technologies.

5.1.1 GDPR outsourcing costs

Introduction of GDPR brought new opportunities of work for outsourcing companies who offer solutions and services related to the Regulation. On the Czech market there are several service providers. Some of them are focused on private businesses and some are

concentrated on private institutions like public authorities and schools. This chapter will analyse the price lists of two GDPR service providers – one focused on public organisations and one private.

Even though the compliance costs represent significant expenses for the organisations, non-complying cost with GDPR is way more devastating since a fine may be granted to the amount of 20 million EUR (or up to 4% of the total worldwide annual turnover in the case of an enterprise).

5.1.1.1 Compliance costs for public organisations

GDPR implementation services for cities and municipalities are provided by the company called SPMO (19). The company offers a wide range of services. The service includes:

- introductory training of city and municipal leaders, project teams and executives,
- methodological management of the implementation of GDPR rules,
- consultation and commenting on collected materials,
- consultation on created documents (analyses, audits, DPIA, etc.),
- consultation on identified processes,
- consultation on proposed procedures for managing personal data processing processes, including designing management procedures,
- input analysis,
- differential analysis and solution proposals,
- specifications identified by processes,
- consultation and integration of privacy standards into general information security rules, and
- training on proposed system of processing and protection of personal data according to GDPR.

The price of GDPR implementation depends on the type of organisation or authority. Price list is summarised in the following table.

Number of employees in organisation	**Municipal authorities** (price excl. VAT per employee)	**Including DPO** (price per month)
100 employees or below	2,500 CZK	3,900 CZK
101 – 200 employees	1,900 CZK	4,900 CZK
201 – 300 employees	1,500 CZK	5,900 CZK
301 – 400 employees	1,300 CZK	6,900 CZK
401 – 500 employees	1,100 CZK	7,900 CZK
500 employees or above	900 CZK	8,900 CZK
Number of employees	**Contributory organisations** (price excl. VAT per organisation)	**Including DPO** (price per month)
Public school facilities	5,000 CZK	500 CZK
Public health facilities	15,000 CZK	500 CZK
Other contributory organisations	9,000 CZK	500 CZK

Table 9 Price list SPMO. Own work, based on https://spmo.cz/gdpr-ochrana-osobnich-udaju/cenik-gdpr-a-naslednych-sluzeb/

The table shows that the implementation cost in a municipal authority with 100 employees can go up to 250,000 CZK. If the price of DPO is also taken into account, then GDPR compliance cost for one year is 296,800 CZK (the price include implementation cost plus twelve times 3,900 CZK). Obviously, the more employees in the authority, the less will be spent for one employee. Implementation cost for an authority with 500 employees is 450,000 CZK. Together with assigning of Data Protection Officer the compliance cost can reach 556,800 CZK (= 500*900 + 12*8,900).

5.1.1.2 Compliance costs for private organisations

Another company, eDPO, focused mainly on private organisations, offers a SW tool for implementing and operating GDPR (20). eDPO allows organisations to start using the application in any state of GDPR implementation. The tool provides effective solutions for organizations, holdings, GDPR implementers, trustees, hospitals, schools, regional authorities, municipalities, local authorities and their contributory organizations.

Among the main features of the application belong, for example:

- assistance in mapping GDPR requirements,
- GDPR implementation wizard,
- input analysis of GDPR compliance,
- personal data security analysis,
- management of consent templates,
- registration of contracts with data processors,
- risk analysis,
- DPIA,
- keeping processing records,
- process mapping,
- and more.

Figure 3 eDPO. Fields of application. Available at: https://www.edpo.cz/#part-8

The price list of the application applies to organizations up to 150 employees. Individual price list is created for the organisations that have more employees. The

application offers four version. Condition for SW license is a purchase for at least one year. The versions are as following:

- **eDPO Single** – for one organisation, templates are included.
- **eDPO Multi** – for one organisation, templates are included, possibility to share already entered data among licensing customers, cannot be used only for one organisation, possibility to enter additional users to customers.
- **eDPO Officer** – for one organisation, templates are included, possibility to share already entered data among Officer licensing customers, cannot be used only for one organisation, without possibility to enter additional users to customers.
- **eDPO Implementer** – for one organisation, templates are included, possibility to share already entered data among Implementer licensing customers, without possibility to enter additional users to customers.

Following table displays costs of the eDPO versions:

eDPO version	**Cost per month**
eDPO Single	1,200 CZK
eDPO Multi	800 CZK
eDPO Officer	600 CZK
eDPO Implementer	1,800 CZK

Table 10 eDPO price list. Available at: https://www.edpo.cz/cenik.html

eDPO also offers legal services and GDPR consultations, which is led by a team of experts. The service is provided for at least six months. Service range is 30 hours per month and the cost for one month is 55,000 CZK.

In case that an organisation with less than 150 employees will buy eDPO Single license for one year and also use the opportunity to have legal services and GDPR consultation, the price for one year will be 674,400 CZK (= 1,200*12 + 55,000*12).

5.1.2 Implementation cost in the selected company

The selected organisation, that was analysed in this thesis, did not use any outsourcing company to implement GDPR. Given the fact, that according to analysis, no DPIA nor DPO is required, the company management has prepared for GDPR itself.

Preparation for GDPR required involvement of managing director, IT manager and accountant.

The biggest share of total costs is the time spent studying the Regulation and aligning organisational and technical measures. Training of employees has not been performed by any third party. Managing director just discussed with employees GDPR requirements, so every employee can be aware of proper personal data protection.

GDPR compliance cost in the selected organisation is summarized in the following table:

Employee	**Charged wage per hour**	**Time spent by studying GDPR and aligning organisational and technical measures**	**Cost**
Director	800 CZK	20 hours	16,000 CZK
IT manager	600 CZK	15 hours	9,000 CZK
Accountant	300 CZK	5 hours	1,500 CZK
Total cost			**26,500 CZK**

Table 11 GDPR compliance cost in the selected organisation. Own work

Evidently, the company did not spend any significant amount of money for the Regulation implementation. According to compliance analysis from practical part all incurred expenditures were sufficient, and the company meets all GDPR requirements.

5.2 GDPR satisfaction survey

Since the end of May, when the EU's General Data Protection Regulation began to apply, the Office for Personal Data Protection has received about 2,300 complaints. People complain mainly about telemarketing and the way they require consent to the processing of personal data. No fines in connection with the Regulation has not been made so far. The Office still waits for a Transformation Act that has not passed the Parliament yet. GDPR applies to public institutions or companies that register their employees, members and customers. It can be assumed that the results of the measures will only be reflected in a longer time.

The Median survey shows that 56 percent of people in the Czech Republic think that GDPR does not help protect sensitive data (14). There is different point of views from

students, employees and entrepreneurs. The Regulation influence not only private entrepreneurs and employers but also public institutions like schools.

In particular, schools have a negative experience in GDPR since it brings more bureaucracy. Teachers have to obtain from parents consent to the processing of children's personal data. That means birthday, place of residence, health insurance, and photos from leisure events on school websites. As some of the parents disagree with posting of children's pictures on the publicly available sites, majority of the websites had to be cancelled.

The graph below shows people's views on whether GDPR helps protect sensitive data. Out of 1017 respondents, 37 percent agree with the Regulation, 56 percent disagree, 7 percent don't have any opinion.

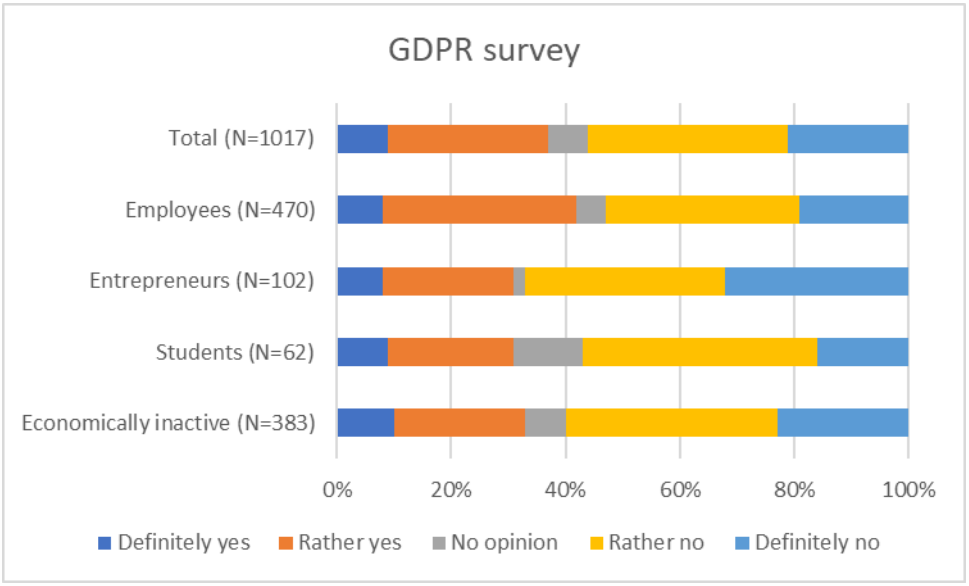

Figure 4 GDPR survey. Available at: https://www.irozhlas.cz/zpravy-domov/gdpr-evropske-narizeni-o-osobnich-udajich-pruzkum-median-cesky-rozhlas_1812270630_jgr

As can be seen at the graph above, there is generally negative opinion about the Regulation. Around one third of entrepreneurs believe that GDPR does not help to protect their sensitive data. The negative assessment from the employers can be caused by increased bureaucracy.

As a possible reason on negative view to GDPR is that people did not perceive this measure well because there was no significant social debate developed in the Czech Republic. From the point of view of an ordinary person, this Regulation appeared from nothing, and perhaps the general assessment it is damaging to the fact that it was adopted on the basis of European Union regulation.

On the other hand, from the point of view of employees, the Regulation is perceived positively. For employees, as one of the most vulnerable groups with regard to the protection of personal data, is the General Data Protection Regulation welcome data protection tool. The aim of the Regulation was to give people more opportunities to protect their rights, which has undoubtedly happened.

Only 10 percent of all respondents stated that GDPR definitely helped to protect their sensitive data. Except of employees, the 22-23 % of respondents from other groups claimed that the Regulation rather helps to protect personal data. Students turned out as the most undecided group – 12 % of them showed no opinion.

As the most important outcome of the survey is the fact that since GDPR is more discussed it has become big media theme, which has greatly increased general awareness, respect and interest in the area of personal data protection.

6 Conclusion

The main goal of this thesis was to analyse GDPR implementation and impacts of the Regulation in a selected organisation. Qualitative method was used for the purposes of the analysis. Using the questionnaire measuring the GDPR compliance it was found that all GDPR requirements were met and the company is compliant. The Data Protection Impact Assessment was conduct for the purposes of the thesis even though it was not required by GDPR.

One of the partial goals was to study a current state and to make a literature review of the personal data protection framework in the European Union. Since the Regulation is quite new, not a lot of hard books have been written yet. However, the Regulation itself contains all important information that is needed for all organisations to comply with GDPR.

Another partial goal was to evaluate possible consequences of GDPR for a selected organisation. There are number of risks that can occur during processing of personal data. Risk assessment has been performed for the reason of evaluating the personal data security risks in the company. As the main risks were identified unauthorised access to personal data, alteration, accidental destruction, unwanted modification of personal data, and loss of personal data. Probability and impact of the risks were calculated using a risk assessment matrix. The majority of identified risks belong to medium risk category. It was recommended to implement proper organisational and technical measures in order to mitigate possible risks.

Since GDPR began to apply, it brings several changes in terms of personal data protection. Clear language has to be used, therefore, privacy policies are written in a clear, straightforward language; the data subject has to give consent to processing of his/her personal data before a business starts with processing; business has to inform the data subject about purpose of the processing and about any transfer of the personal data; the data subject has more rights, for example right to erasure, right to access the data and right to be informed in case of data breach. Since GDPR is more discussed it has become big media theme, which has greatly increased general awareness, respect and interest in the area of personal data protection.

Being an EU Regulation the GDPR is directly applicable in all EU countries. However, it also requires countries to adapt their national legislation. As of January 2019,

23 Member States have adopted the required national legislation, five are still in the process of doing so (Bulgaria, Greece, Slovenia, Portugal, Czech Republic). Since the national legislation has not been implemented in the Czech Republic yet, no fines in connection with the Regulation has not been made so far. The Office for Personal Data Protection still waits for a transformation act on personal data processing, that has not passed the Parliament yet.

7 References

1. **Eurlex.cz.** *Directive 95/46/ES.* [online, accessed 22 Mar. 2018] Available at: http://www.eurlex.cz/dokument.aspx?celex=31995L0046
2. **NEZMAR, Luděk.** *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
3. **ŽŮREK, Jiří**. *Praktický průvodce GDPR.* Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.
4. **The office for personal data protection.** *GDPR (General Regulation).* [online, accessed 24 Mar. 2018] Available at: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938
5. **The office for personal data protection.** *GDPR obligations.* [online, accessed 24 Mar. 2018] Available at: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938
6. **The office for personal data protection.** *Rights of the data subject.* [online, accessed 24 Mar. 2018] Available at: https://www.uoou.cz/6-prava-subjektu-udaj/d-27276
7. **The office for personal data protection.** *Sanctions.* [online, accessed 25 Mar. 2018] Available at: https://www.uoou.cz/11-sankce-pokuty/d-27287
8. EU general data protection regulation (GDPR): an implementation and compliance guide. IT governance privacy team. ISBN 9781849288354.
9. **Amir M. Hormozi** (2005) *Cookies and Privacy*, EDPACS, 32:9, 1-13, DOI: 10.1201/1079/45030.32.9.20050301/86855.1
10. ISO 27001:2013, *Technical guidance for transitioning from ISO/IEC 27001:2005* (January 2015)
11. **Quality Austria**. *GDPR ve vztahu k ISO 27001*. [online, accessed 6 Oct. 2018] Available at: https://www.qualityaustria.cz/gdpr-ve-vztahu-k-iso-27001
12. **EUGDPR.org.** *Timeline of events*. [online, accessed 15 Sept. 2018] Available at: https://eugdpr.org/the-process/timeline-of-events/
13. ISO 31000:2018, *Risk management guidance*. [online, accessed 20 Dec 2018] Available at: https://www.iso.org/iso-31000-risk-management.html
14. **Median agency**. *GDPR Survey*. [online, accessed 20 Dec 2018] Available at: https://www.irozhlas.cz/zpravy-domov/gdpr-evropske-narizeni-o-osobnich-udajich-pruzkum-median-cesky-rozhlas_1812270630_jgr

15. **Workiva.** *Building a risk assessment.* [online, accessed 5 Jan 2019] Available at: https://www.workiva.com/blog/building-risk-assessment-matrix
16. **Bitkom**. *Risk assessment and Data Protection Impact Assessment guide*. [online, accessed 5 Jan 2019] Available at: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf
17. **Ministerstvo zdravotnictví ČR.** *Metodika implementace ve zdravotnictví.* [online, accesed 15 Dec 2018]. Available at: https://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr_14864_3805_11.html
18. **Securitymetrics.com**. *How much does GDPR compliance cost?* [online, accessed 28, Feb 2019]. Available at: https://www.securitymetrics.com/blog/how-much-does-gdpr-compliance-cost
19. **SPMO**. *GDPR implementation price list.* [online, accessed 3, Mar 2019]. Available at: https://spmo.cz/gdpr-ochrana-osobnich-udaju/cenik-gdpr-a-naslednych-sluzeb/
20. **eDPO**. *SW for GDPR implementation*. [online, accessed 3, Mar 2019]. Available at: https://www.edpo.cz/#part-1