

Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology



**Česká zemědělská
univerzita v Praze**

Bachelor Thesis

GDPR Compliance check on an e-commerce website.

Bharvi Desai

© 2023 CULS Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Bharvi Kalpesh Desai, BSc

Informatics

Thesis title

GDPR Compliance check on an e-commerce website.

Objectives of thesis

The main object of the thesis is the inspection of fitness007.cz, an e-commerce platform that sells sports goods and fitness equipment for its GDPR compliance. This research will include a literature review of the General Data Protection Regulation (GDPR) and its principles. The inspection will be done on the basis of Risk, Security, Consent, and Transparency analysis. Our secondary objective is to provide the platform with a report on its current compliance status with recommendations to reach best practice compliance from basic and minimum compliance.

Methodology

1. Learning about GDPR Principles: Principles include consent from the user, privacy policy being clear and easily accessible, securing the user data, and maintaining confidentiality.
2. Reviewing E-commerce website: Verifying its privacy policy, terms & conditions, and other relevant documents that fall under the data collection and processing category.
3. Identifying the information gathered: Personal data the website collects like name, email address, shipping address, payment information, etc.
4. Checking for consent: Verifying whether the website is gaining user consent for the gathering and processing of their personal data. To obtain user consent, there can be checkboxes, opt-in forms, or other mechanisms.
5. Checking for transparency: Verifying if it makes its data collecting and processing procedures explicit and easily available. Check for disclosures that describe how user data is used and shared, such as privacy policies, cookie notices, and other such clauses.
6. Checking for User Rights: Verifying that users are able to utilize their GDPR rights, such as the right to access their data, the right to have inaccurate data corrected, and the right to have their data erased.
7. Data breach Response plan: Going through the company's Data breach response plan if there is any.
8. Analysing: From all the above-gathered information, evaluate and summarise the GDPR compliance of the website.

9. Making suggestions to the website owners or the users: Give the website owners recommendations to improve GDPR compliance based on my study. It could be updating the privacy policy, adding security measures, or providing clearer terms.



The proposed extent of the thesis

40

Keywords

GDPR , Personal data, Data processing, Data protection, Data privacy, Customer data, Data security, Privacy policy, Cookie Policy, Consent , Data controller, Data processor, PEF-CULS

Recommended information sources

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

<https://gdpr.eu/>

IT Governance Publishing. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. 1st edition. 2017. ISBN 978-1-84928-982-9

Watkins, S. G. ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. 2nd edition. 2016. ISBN 978-1-84928-714-6

Expected date of thesis defence

2021/22 SS – FEM

The Bachelor Thesis Supervisor

Ing. Jakub Konopásek, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 7. 3. 2023

Ing. Martin Pelikán, Ph.D.

Head of department

Electronic approval: 13. 3. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 15. 03. 2023

Declaration

I declare that I have worked on my bachelor thesis titled "GDPR Compliance check on an e-commerce website" by myself and I have used only the sources mentioned at the end of the thesis. As the author of this bachelor thesis, I declare that the thesis does not break copyrights of any other person.

In Prague on 15.3.2023

Acknowledgement

I would like to thank Ing. Jakub Konopásek, Ph.D. for his advice and support during my work on this thesis.

GDPR Compliance check on an e-commerce website.

Abstract

This thesis is focused on examining how well fitness007.cz, an e-commerce website that sells sports goods and fitness equipment, is following the GDPR rules. To do this, the thesis will review the GDPR principles, and then analyse the platform's compliance in terms of risk, security, consent, and transparency. The goal of the study is to create a report that shows the current level of compliance of the platform, along with suggestions for improving it. The research will involve looking at the platform's privacy policy, terms & conditions, and other documents that relate to how it collects and processes data. Additionally, the study will determine whether the platform provides clear information about its data collection and processing procedures, user rights, and plan for responding to data breaches. Finally, the research will evaluate the platform's GDPR compliance and provide recommendations for how to enhance it.

Keywords

GDPR, Personal Data, User consent, Data subject, Controller, User rights, Data breaches, Privacy policy, Data Protection, Data Security

Kontrola souladu s GDPR na webu elektronického obchodu.

Abstraktní

Tato práce je zaměřena na zkoumání toho, jak dobře dodržuje pravidla GDPR fitness007.cz, e-shop, který prodává sportovní zboží a fitness vybavení. Za tímto účelem práce přezkoumá principy GDPR a poté analyzuje soulad platformy z hlediska rizika, zabezpečení, souhlasu a transparentnosti. Cílem studie je vytvořit zprávu, která ukazuje aktuální úroveň souladu platformy spolu s návrhy na její zlepšení. Výzkum bude zahrnovat prozkoumání zásad ochrany osobních údajů, podmínek a podmínek platformy a dalších dokumentů, které se týkají toho, jak shromažďuje a zpracovává data. Studie navíc určí, zda platforma poskytuje jasné informace o svých postupech shromažďování a zpracování dat, uživatelských právech a plánu reakce na narušení dat. Nakonec výzkum vyhodnotí soulad platformy s GDPR a poskytne doporučení, jak jej zlepšit.

Klíčová slova

GDPR, Osobní údaje, Souhlas uživatele, Subjekt údajů, Správce, Uživatelská práva, Porušení ochrany osobních údajů, Ochrana osobních údajů, Zabezpečení údajů

Contents

1. Introduction	9
2. Objectives and Methodology	10
2.1. Objective	10
2.2. Methodology	10
3. Literature Review	11
3.1. Scope	11
3.2. Glossary	12
3.3. Principles of GDPR	13
3.4. Rights of the Data Subject	15
3.5. Controllers and Processors	17
3.6. Transfer of personal Data to third party countries or international organization	18
3.7. Independent Supervisory Authorities	19
3.8. Cooperation and Consistency	19
3.9. European Data Protection Board	20
3.10. Remedies, Liabilities and Penalties	21
3.11. Delegated Acts & Implementing Acts	23
3.12. Final Provision	24
4. Practical Part	25
4.1. Company Introduction	25
4.2. Scope of the Investigation	25
4.3. Survey	26
4.3.1. Review of the website's policies	26
4.3.2. Survey Questionnaire	26
4.4. Risk Assessment	32
5. Results & Discussion	35
5.1. Recommendations	37
5.2. Limitations	38
6. Conclusion	39
7. References	40

1. Introduction

In the 1970s, concerns about privacy emerged due to the increased use of computers to process personal information and cross-border trade that led to the sharing of personal data (Witzleb et al., 2019). To address this, privacy standards were needed that could balance the protection of privacy and free trade facilitation. The Universal Declaration of Human Rights and the European Convention for the protection of human rights served as starting points, recognizing personal rights that were not absolute (Marelli, 2018).

The first harmonization of privacy laws in Europe came about due to EU resolutions 73/22 and 74/29, which were followed by the OECD guidelines in 1980 (Marelli, 2018). The Council of Europe approved convention 108 in 1981, which became the first international legal instrument for data protection (Witzleb et al., 2019). This convention prohibited the handling of personal information such as racial, political opinions, health, or criminal convictions. The Data Protection Directive of 1995 brought about reharmonization of privacy legislation but also led to differences because a directive is not directly binding on all European countries (Witzleb et al., 2019). To address this issue, the European Commission worked on the GDPR between 2009 and 2016, which laid down a single set of binding rules across the EU (EU, 2016).

The GDPR, a vast network of regulations enacted by the European Union (EU) and the European Economic Area (EEA), affords extensive safeguarding of personal data collected from individuals within these regions. This piece of legislation lays a strong focus on preserving the highest standards of privacy, openness, accuracy, and accessibility. Its thorough structure strives to guarantee that personal facts are exclusively gathered, handled, or managed upon explicit approval so as not to infringe on any person's entitlement to privacy. The stated legislation defines distinct requirements for the management and safeguarding of personal data, including any transfer or transportation of said information outside the boundaries of EU and EEA nations. The regulation's main goal is to provide people more privacy and control over their personal data. Recognizing GDPR's all-encompassing and extensive effects would be a significant accomplishment. This global law has effects that cut across national boundaries and legal jurisdictions. No matter where they are physically located, it covers any organization in charge of sensitive data pertaining to citizens of the EEA or EU. (EU)

2. Objectives and Methodology

2.1. Objective

The main object of the thesis is the inspection of fitness007.cz, an e-commerce platform that sells sports goods and fitness equipment for its GDPR compliance. This research will include a literature review of the General Data Protection Regulation (GDPR) and its principles. The inspection will be done based on Risk, Security, Consent, and Transparency analysis. Our secondary objective is to provide the platform with a report on its current compliance status with recommendations to reach best practice compliance from basic and minimum compliance.

2.2. Methodology

This methodology outlines a process to evaluate the General Data Protection Regulation (GDPR) compliance of an e-commerce website. The process includes eight steps, starting with understanding GDPR principles such as obtaining user consent and maintaining confidentiality. It then involves reviewing the website's privacy policy and terms & conditions and identifying the personal data collected. The next step is to verify whether the website is transparent in its data collection and processing procedures and whether it allows users to exercise their GDPR rights. It also involves checking the company's data breach response plan if they have it published. Finally, the gathered information is analysed to evaluate the GDPR compliance of the website, and recommendations are provided to improve compliance. The recommendations may include updating the privacy policy, adding security measures, or providing clearer terms.

3. Literature Review

The General Data Protection Regulation (GDPR) was implemented in May 2018 and is known as Regulation (EU) 2016/679 of the European Parliament and Council. This all-encompassing regulation aims to uphold privacy for EU citizens by enforcing strict guidelines on how personal data can be stored, collected, processed or transferred. Application-wise it applies not only to any organization within the EU that processes this kind of information but also non-EU organizations providing a service or product while collecting such data from an EU citizen/clientele base. The implementation reflects update requirements considering changes in digital trends with greater transparency measures being put into place along with higher levels of accountability related to control over dissemination protocols regarding personal data (European Union, 2016).

3.1. Scope

This regulation applies to:

- The processing of personal data by a controller or processor established in the Union, regardless of whether the processing occurs within the Union or not (EU General Data Protection Regulation, Art. 3(1)).
- The processing of personal data of individuals in the Union by a controller or processor (not established) in the Union if the processing is related to offering goods or services to these individuals within the Union or monitoring their behaviour if it occurs within the Union (EU General Data Protection Regulation, Art. 3(2)).
- The processing of personal data by a controller who is not based in the Union but is situated in a country where Member State law is applicable as a result of public International law (EU General Data Protection Regulation, Art. 3(2)).

This regulation applies to how personal information is used by computers or in files.

However, there are some situations where it doesn't apply, such as when personal data is used for personal or household activities, or by authorities for criminal investigations (EU General Data Protection Regulation, Recital 18).

If the European Union (EU) uses personal data, they must follow a different regulation. And if they use the personal data of people who are not in the EU, they may still need to follow this regulation if they offer goods or services to people in the EU or monitor their online behaviour (EU General Data Protection Regulation, Art. 3(2)).

3.2. Glossary

- **'Data subject'** is an individual person, who is either identified or identifiable and whose personal data is being processed by a controller or processor. An identifiable natural person means a person who can be identified, either directly or indirectly, through an identifier such as a name, identification number, location data, online identifier, or by one or more specific factors relating to their physical, physiological, genetic, mental, economic, cultural, or social identity (GDPR, 2016, art. 4, para. 1).
- **'Personal data'** refers to any details concerning an identified or identifiable individual ('**data subject**') (GDPR, 2016, art. 4, para. 1).
- **'Processing'** refers to any action or series of actions carried out on personal data, either manually or automatically. These actions include the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other forms of provision, alignment or combination, limitation, erasure or destruction of personal data or a set of personal data (GDPR, 2016, art. 4, para. 2).
- **'Profiling'** refers to any automated handling of personal data that assesses specific aspects of an individual, primarily to scrutinize or anticipate the performance, financial position, health, personal choices, inclinations, reliability, behaviour, whereabouts, or travel movements of that individual (GDPR, 2016, art. 4, para. 4).
- **'Controller'** refers to an individual or organization, whether it is a public authority, agency, or other body, that decides on its own or with others, the purposes and methods of processing personal data. The law of the Union or the Member State governs the processing of personal data, and it may also specify the controller's appointment process or specific eligibility requirements (GDPR, 2016, art. 4, para. 7).
- **'Processor'** refers to an individual or organization that carries out the processing of personal data on behalf of the controller (GDPR, 2016, art. 4, para. 8).

- **‘Third party’** refers to any individual or organization, including a public authority, agency, or body, that is not the data subject, controller, processor, or individuals authorized by the controller or processor to process personal data under their direct supervision. The 'consent' of the data subject means an explicit, informed, freely given, and unambiguous indication of the data subject's preferences, through a clear affirmative action or statement, agreeing to process personal data (GDPR, 2016, art. 4, para. 10).
- **‘Consent’** refers to the expression of the data subject's wishes, which should be freely given, specific, informed, and unambiguous. This can be indicated by a statement or a clear affirmative action that shows agreement to the processing of personal data related to them (GDPR, 2016, art. 4, para. 11).
- **‘Personal data breach’** refers to a security breach that results in the accidental or unlawful destruction, loss, modification, unauthorized access, or disclosure of personal data that is being transmitted, stored, or otherwise processed (GDPR, 2016, art. 4, para. 12).

3.3. Principles of GDPR

I. Lawfulness, fairness, and transparency: It is of utmost importance to adhere to the foundational principle set forth by GDPR, which mandates that any handling or processing of personal data must be executed in a manner consistent with upholding legality, impartiality and transparency. Such compliance ensures respect for individual privacy and adherence to ethical standards within organizations responsible for managing sensitive information. The recipient should be notified about why their information is being processed, what pieces would undergo processing, and the lawful rationale behind it. Furthermore, fairness necessitates considering a user's rights and benefits while administering said procedure to them (GDPR, 2016, Art. 5, para. 1a).

II. Purpose limitation: The second principle of the GDPR states that the personal data has to be collected for specified, explicit, and legitimate purposes. It is indicated that the individual responsible for managing data must furnish a lucid and tangible justification of their collection endeavours, with strict guidelines prohibiting its utilization outside those

confines unless granted express permission from the party whose information it pertains to (GDPR, 2016, Art. 5, para. 1b).

III. Data minimization: The third principle of the GDPR states that the personal data has to be adequate, relevant, and limited to what is necessary for processing, reason being specified. It is of critical importance that the individual or organization tasked with managing data only procures information that serves an explicitly defined purpose and refrains from acquiring superfluous details beyond what is essential. (GDPR, 2016, Art. 5, para. 1c)

IV. Accuracy: The fourth principle of the GDPR states that the personal data has to be accurate and, be kept up to date. This means that the data controller must take reasonable steps to ensure that the data is accurate and update if required and necessary (GDPR, 2016, Art. 5, para. 1d).

V. Storage limitation: The limitation of storage is a crucial aspect of the General Data Protection Regulation's fifth principle. In essence, this regulation requires that personal data should only be kept for as long as it serves its intended purpose in identifying relevant parties. It may, however, continue to exist beyond this point if there are specific reasons related to archives, public interest research or statistics - provided appropriate technical and organizational measures have been taken to secure rights and freedoms attached thereto. (GDPR, 2016, Art. 5, para. 1e)

VI. Integrity and confidentiality: The sixth principle of the GDPR states that the personal data must be managed in a way that guarantees suitable security measures are in place to prevent unauthorized or illegal processing, accidental loss, destruction, or damage, by using appropriate technical or organizational strategies (GDPR, 2016, Art. 5, para. 1f).

VII. Accountability: The GDPR's seventh principle notes that responsibility lies with the data controller for upholding compliance. This entails being able to prove such conformity while maintaining detailed logs of processing activities. The appointment of a data

protection officer is also mandatory if necessary, and prompt reporting regarding any breaches must be made known to supervisory authorities (GDPR, 2016, Art. 5, para. 2).

3.4. Rights of the Data Subject

- **Right to be informed**

One of the fundamental rights protected by the GDPR is the right to information. Organizations must disclose how they utilize personal data in a transparent manner. Particularly, data subjects have a right to information about what personal data is processed, its purpose, who is it shared with, and how long it will be kept (ICO, 2018, para. 12).

The disclosure of this information to data subjects by organizations must be concise and easily understood, it is usually in the form of a privacy notice (GDPR, 2016, Article 12). While collecting personal information, or as soon as is practical after, the privacy notice should be made available and easily accessible (GDPR, 2016, Article 13).

- **Right to access**

Data subjects are entitled to the right of access. Such provision enables them to retrieve and obtain a copy of their personal data, which includes information on the purposes of data processing, the types of personal data that are being processed, and the recipients of the data. If a data subject wants access to this crucial information, they can ask for it verbally or in writing (GDPR, 2016, Art. 15).

Organizations are required to respond to the request within one month and provide the requested information free of charge (GDPR, 2016, Art. 15, para. 1).

- **Right to rectification**

The right to rectification gives data subjects the right to request that inaccurate or incomplete personal data is corrected. This means that data subjects can request that organizations update or change their personal data if it is incorrect or out of date (EU, 2016, art. 16).

Organizations must respond to requests for rectification within one month. If the personal data has been shared with third parties, the organization must inform them of the rectification request and ensure that the personal data is updated accordingly (GDPR, 2016, Art. 16, para. 3).

- **Right to erasure**

Data subjects have the option to ask for the deletion of their personal information under the right to erasure, often known as the "right to be forgotten." (GDPR, 2016, Article 17). This right is not absolute, and organizations may be able to refuse a request for erasure in certain circumstances. For example, if the personal data is required for legal or regulatory purposes (ICO, 2020, para. 28).

Requests for erasure must be answered by organizations within a month. If the sensitive information has accidentally been disclosed to third parties without your knowledge, it is the data controller's duty to inform them and to ensure the complete deletion of the offending documents. (GDPR, para. 17).

- **Right to restrict processing**

The right to restrict processing gives data subjects the right to request that the processing of their personal data be restricted in certain circumstances. For example, if the personal data is inaccurate or the processing is unlawful (GDPR, 2016, Art. 18).

Organizations must respond to requests for restriction within one month. If the personal data has been shared with third parties, the organization must inform them of the restriction request and ensure that the personal data is processed accordingly (The GDPR, n.d., para. 18).

- **Right to data portability**

The right to data portability gives data subjects the right to receive their personal data in a structured, commonly used and machine-readable format, and to transmit it to another controller without hindrance (GDPR, 2016, Article 20).

This right only applies to personal data that has been provided by the data subject to the organization, and where the processing is based on consent or a contract. Organizations must respond to requests for data portability within one month (The GDPR, para. 20).

- **Right to object**

The right to object gives data subjects the right to object to the processing of their personal data in certain circumstances. This includes where the processing is based on legitimate interests, or for direct marketing purposes (GDPR, para. 21).

Organizations must respond to requests for objection within one month. If the personal data is being processed for direct marketing purposes, the organization must stop processing the personal data immediately (GDPR, 2016, Art. 21).

- **Rights related to automated decision making.**

Rights related to automated decision making refer to the rights of data subjects in situations where decisions are made about them solely by automated means, without any human involvement. This is commonly referred to as "automated decision making" or "profiling" (ICO, 2020, para. 4).

3.5. Controllers and Processors

Controllers and processors have specific obligations and responsibilities when it comes to handling personal data. Controllers are responsible for ensuring that they only work with processors who can provide sufficient guarantees regarding data protection and must ensure that contracts with processors contain certain provisions related to data protection (GDPR, 2016, Art. 28). Processors must also adhere to several requirements, such as ensuring that they only process personal data in accordance with the controller's instructions and putting in place the necessary organizational and technical safeguards to protect the security of personal data (GDPR, 2016, Art. 32). Both controllers and processors must report any personal data breaches to the supervisory authority within 72 hours of becoming aware of the breach (GDPR, 2016, Art. 33).

According to the GDPR, data subjects have the right to hold both controllers and processors accountable for any violations of the law. The severity of the fines and

punishments means that organizations that violate them will suffer serious consequences. Hence, it is crucial that all parties involved, whether they are the controller or the processor, understand their duties under this mandate; appropriate measures must then be taken as necessary towards meeting regulatory expectations (The GDPR, 2016).

3.6. Transfer of personal Data to third party countries or international organization

The transfer of personal data to third countries or international organizations is subject to strict requirements and can only take place if the transfer meets certain conditions specified in the GDPR (GDPR, n.d., para. 46).

These conditions include:

Adequacy decision: The European Commission may determine that a third country or international organization ensures an adequate level of data protection that is comparable to that provided by the GDPR. If an adequacy decision is made, personal data may be transferred to that country or organization without further safeguards being necessary (GDPR, n.d., para. 47).

Appropriate safeguards: If no adequacy decision has been made, the controller or processor may still transfer personal data to a third country or international organization if they provide appropriate safeguards to protect the data. These safeguards may include binding corporate rules, standard contractual clauses, or other approved mechanisms (GDPR, n.d., para. 48).

Derogations: In certain limited circumstances, personal data may be transferred to a third country or international organization without meeting the adequacy or appropriate safeguards requirements. These circumstances include situations where the data subject has provided explicit consent, where the transfer is necessary for the performance of a contract,

or where the transfer is necessary for important reasons of public interest (GDPR, n.d., para. 49).

3.7. Independent Supervisory Authorities

The European Union member states have set up independent supervisory authorities, like the Information Commissioner's Office (ICO) of the UK. Their main goal is to enforce and safeguard people's rights when it comes to their personal data in accordance with the General Data Protection Regulation (GDPR). These entities carry out various tasks such as keeping watch for potential violations of GDPR provisions, giving advice and support both individuals and organizations can rely on while punishing those who do not comply through imposition fines. The cooperative work among these bodies guarantees a uniform application of GDPR throughout EU countries which holds an essential role in promoting privacy protection measures concerning individual information security (ICO 2021 line 1-3).

3.8. Cooperation and Consistency

The General Data Protection Regulation (GDPR) is upheld by the fundamental principles of cooperation and consistency, which were specifically designed to promote unvarying application throughout all member states within the European Union while also emphasizing joint efforts from data protection authorities (DPAs) in executing their duty to enforce GDPR's provisions (GDPR, 2016, Recital 17).

Cooperation: The act of cooperation relates to the coordination and collaboration between DPAs and different relevant governing entities within various EU member states, especially when resolving cross-border data protection issues. In order to ensure uniform implementation of legislation across all member states, the GDPR requires DPAs to cooperate with one another and share information. Collaboration can take many different forms, including joint investigations, intelligence sharing, and assistance measures that are given in exchange (GDPR, 2016, Article 60).

Consistency: On the other hand, we have consistency. This relates to applying GDPR consistently throughout all EU member states. No matter who they are or where they handle their information, GDPR aims to ensure that everyone has the same rights to data privacy. In order to achieve this goal, the European Data Protection Board (EDPB) was established under the GDPR's purview. The EDPB ensures uniform application across the nations under its supervisory authority by providing guidance and other pertinent advice to DPAs, as well as, if necessary, mediating disputes between them (GDPR, 2016, Article 63).

To ensure effective application of the GDPR and protection of individuals' data privacy rights, cooperation and consistency are crucial. DPAs working in tandem while maintaining consistent standards can guarantee that organizations adhere to the regulations outlined by GDPR, impart confidence among individual users about how their personal information is being managed (GDPR, 2016, Recital 17) .

3.9. European Data Protection Board

The European Data Protection Board (EDPB) is an independent body established by the General Data Protection Regulation (GDPR) to ensure consistent application of data protection rules across the European Union (EU). The EDPB is composed of representatives from each EU member state's national data protection authority (DPA), as well as the European Data Protection Supervisor (GDPR, Art. 68, para. 1 & 2).

The primary role of the EDPB is to promote the consistent application and interpretation of the GDPR across the EU (GDPR, Art. 70, para. 1). To achieve this, the EDPB provides guidance and advice to DPAs, as well as to individuals and organizations, on how to interpret and comply with the GDPR. The EDPB also issues binding decisions in certain cases, such as when there is disagreement between DPAs on how to apply the GDPR in a specific situation (GDPR, Art. 65, para. 1).

The EDPB has several specific tasks and responsibilities, including:

1. Providing advice and guidance to the European Commission on data protection matters (GDPR, Art. 70, para. 1).

2. Issuing guidelines on the interpretation and application of the GDPR (GDPR, Art. 70, para. 1).
3. Promoting cooperation between DPAs and other relevant authorities across the EU (source, GDPR, Art. 70, para. 1).
4. Mediating disputes between DPAs, particularly in cases where there is disagreement over the interpretation or application of the GDPR (GDPR, Art. 65, para. 1).
5. Promoting awareness of data protection rights and responsibilities among individuals and organizations across the EU (GDPR, Art. 70, para. 1).

The European Data Protection Board (EDPB) has a fundamental responsibility in ensuring the consistent implementation of GDPR regulations throughout all EU nations. It is vital that individuals' data privacy rights are safeguarded, and this can only be achieved through proper guidance provided by EDPB to DPAs, organizations as well as members of the public. Through these efforts, there is increased awareness about essential aspects of data protection which results in upholding uniformity regarding interpretation and application across Europe's jurisdictions (European Data Protection Board, para. 1) .

3.10. Remedies, Liabilities and Penalties

The General Data Protection Regulation (GDPR) provides for a range of remedies, liabilities, and penalties to ensure that organizations comply with the regulation and individuals' data protection rights are protected.

Remedies:

Under the GDPR, individuals have the right to obtain various remedies if their data protection rights have been violated. These remedies may include:

- The right to information regarding the use of their personal data (European Parliament, Council of the European Union, 2016, Art. 13).
- The right to access the personal data that is stored by an organization (European Parliament, Council of the European Union, 2016, Art. 15).

- The right to have inaccurate personal information fixed (European Parliament, Council of the European Union, 2016, Art. 16).
- The right to request the removal of their personal information (also known as the right to be forgotten) (European Parliament, Council of the European Union, 2016, Art. 17).
- The right to limit how their personal data is processed (European Parliament, Council of the European Union, 2016, Art. 18).
- The right to data portability (the right to receive a copy of their personal data in a machine-readable format) (European Parliament, Council of the European Union, 2016, Art. 20).
- The right to express disagreement with the processing of personal data (European Parliament, Council of the European Union, 2016, Art. 21).
- The right to make a formal report to a regulatory body (European Parliament, Council of the European Union, 2016, Art. 77).

Liabilities:

Under the GDPR, organizations that process personal data are liable for any breaches of the regulation (GDPR, 2016, Art. 83). This means that they may be held responsible for any damages caused by their non-compliance, including:

- Financial losses suffered by individuals as a result of a breach (European Parliament, Council of the European Union, 2016, Art. 82).
- Damage to individuals' reputation or privacy (European Parliament, Council of the European Union, 2016, Art. 82).
- Non-material damage such as emotional distress (European Parliament, Council of the European Union, 2016, Art. 82).

Penalties:

The GDPR provides for a range of penalties for non-compliance with the regulation, including:

- Fines of up to €20 million or 4% of global annual turnover, whichever is greater (European Parliament, Council of the European Union, 2016, Art. 83).

- Fines of up to €10 million or 2% of global annual turnover, whichever is greater, for less serious violations (European Parliament, Council of the European Union, 2016, Art. 83).
- Warnings and reprimands (European Parliament, Council of the European Union, 2016, Art. 58).
- Orders to suspend or restrict data processing activities (European Parliament, Council of the European Union, 2016, Art. 58).
- Orders to delete or correct personal data (European Parliament, Council of the European Union, 2016, Art. 58).
- Bans on data processing activities (European Parliament, Council of the European Union, 2016, Art. 58).

The specific penalties imposed will depend on the severity of the violation and other factors, such as the organization's cooperation with authorities and any previous breaches. It is important to note that penalties can be imposed on both controllers (organizations that determine the purposes and means of processing personal data) and processors (organizations that process personal data on behalf) (European Parliament, Council of the European Union, 2016, Art. 82).

3.11. Delegated Acts & Implementing Acts

Delegated acts are defined as "non-legislative acts that supplement or amend the provisions of an existing EU legislative act" (European Union, 2016, para. 1). They are prepared by the European Commission and require approval by the European Parliament and the Council of the European Union. Delegated acts can modify the provisions of the primary legislation, but they cannot change its overall scope or purpose (European Commission, para. 2).

Implementing acts are also non-legislative acts that supplement the provisions of EU legislative acts (European Union, 2016, para. 2). They are prepared by the European Commission and provide detailed technical or administrative rules that are necessary for the effective implementation of EU law. Implementing acts do not require approval by the

European Parliament or the Council of the European Union but are subject to scrutiny by these bodies (European Commission, para. 2).

Both types of acts are used to specify and supplement primary legislation. While delegated acts modify existing provisions, implementing acts provide further clarification and detail. Both types of acts are subject to oversight and scrutiny by the European Parliament and the Council of the European Union (European Union, 2016, paras. 1-3).

3.12. Final Provision

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Art. 99).

The Final Provision of the General Data Protection Regulation (GDPR) is the concluding section of the regulation that contains several miscellaneous provisions (GDPR, 2016).

Firstly, it requires the European Commission to review and report on the application and effectiveness of the GDPR every four years, starting from May 2020, to ensure that it remains relevant and effective in protecting individuals' personal data rights (European Parliament and Council of the European Union, 2016, Art. 97).

Secondly, it establishes the European Data Protection Board (EDPB) as the independent supervisory authority responsible for ensuring consistent application and interpretation of the GDPR throughout the European Union (EU) (European Parliament and Council of the European Union, 2016, Art. 68).

Thirdly, the Final Provision states that the GDPR repeals the previous Data Protection Directive (95/46/EC) and sets out the relationship between the GDPR and other EU laws and regulations, such as the e-Privacy Regulation (European Parliament and Council of the European Union, 2016, Art. 99).

Fourthly, it requires all EU member states to implement and enforce the GDPR and outlines the penalties for non-compliance (European Parliament and Council of the European Union, 2016, Art. 99).

Finally, the Final Provision includes provisions for the regulation's entry into force and its application to certain types of data processing activities that occurred before its effective date (European Parliament and Council of the European Union, 2016, Art. 99).

Overall, the Final Provision of the GDPR aims to ensure that the regulation is properly implemented and enforced throughout the EU and that individuals' personal data rights are protected (European Parliament and Council of the European Union, 2016, Art. 99).

4. Practical Part

This section of the thesis examines fitness007.cz for its compliance with GDPR.

4.1. Company Introduction

Fitness007.cz is a Czech-based fitness company that offers a range of fitness equipment, supplements, and accessories for sale online.

The business was founded in 2013 and has since emerged as the Czech Republic's online fitness goods seller. Dumbbells, weights, benches, and exercise cycles are among the company's product offerings, along with vitamins and athletic apparel. Fitness007.cz takes pleasure in providing premium goods from reliable manufacturers at affordable costs.

Fitness007.cz also has a physical store in Prague where clients may examine and buy items in addition to its online store. Also, the business provides delivery services throughout Slovakia and the Czech Republic.

4.2. Scope of the Investigation

The GDPR compliance of the website is being examined to determine if the website complies with EU laws on the collection and storage of personal data. The investigation's goal is to find any possible gaps or GDPR violations on the website and offer suggestions

for improvement. Examining the website's data protection rules, practices, and data subject rights are all part of the study. During this examination, information will be gathered on the categories of personal data being collected, the legal justification for processing this data, and the security precautions used to safeguard this data.

The overall goal of the investigation is to evaluate the website's compliance with GDPR regulations, identify any areas of improvement, and provide recommendations to ensure the website is transparent, secure, and respects the rights of data subjects.

4.3. Survey

This section of the thesis answers questions about websites privacy policies and its adherence to it

4.3.1. Review of the website's policies

The protection of users' personal information by the organization is outlined in the data safety regulations found on <https://www.fitness007.cz/>. These guidelines states that individuals are notified about any collected data and its intended usage. Additionally, personal details will only be gathered for legitimate purposes. The enterprise also assures clients that they will take organizational and technical precautions to prevent unauthorized processing or manipulation of private records while ensuring their accuracy. Users have several rights under these rules including access to updating their own data as well as objecting to further collection in some cases.

4.3.2. Survey Questionnaire

The subsequent step is to address several review questions concerning the data protection policies of the website. This will involve a critical analysis of the website's data protection policies and their adherence to the principles outlined in the General Data Protection Regulation (GDPR). Additionally, I will provide insights into my personal experience using the website, including any concerns or issues related to data protection and privacy. Overall, this questionnaire aims to

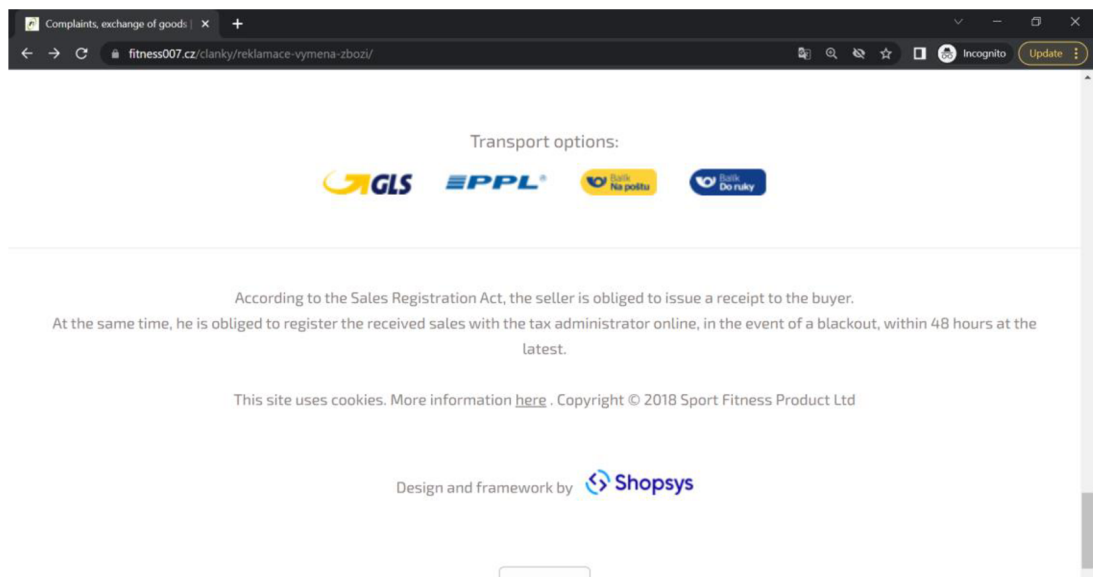
provide a comprehensive assessment of the website's data protection policies and their impact on the user experience, based on publicly available information.

1. Is there a clear and concise explanation of how the website uses cookies and user consent mechanisms to obtain valid consent for data collection? (figure 1)

The online platform does provide a clear and concise disclosure of how it uses cookies and follows an ethical standard while collecting user information. Also, the website's privacy statement provides information on how user consent is obtained. This especially relates to the collection and management of personal data. This requirement states that users must give genuine consent for the collection and management of their personal information while maintaining full control over the decision to revoke such consent at any time. The website states that users will be informed of the best ways to recall such permissions at any time through appropriate procedures put in place by us for assistance-only.

According to the available data, it appears that <https://www.fitness007.cz/> gives comprehensive and understandable descriptions of how the website utilizes cookies and user consent procedures to secure valid consent for data collection in line with GDPR regulations.

Figure 1 Cookies Statement

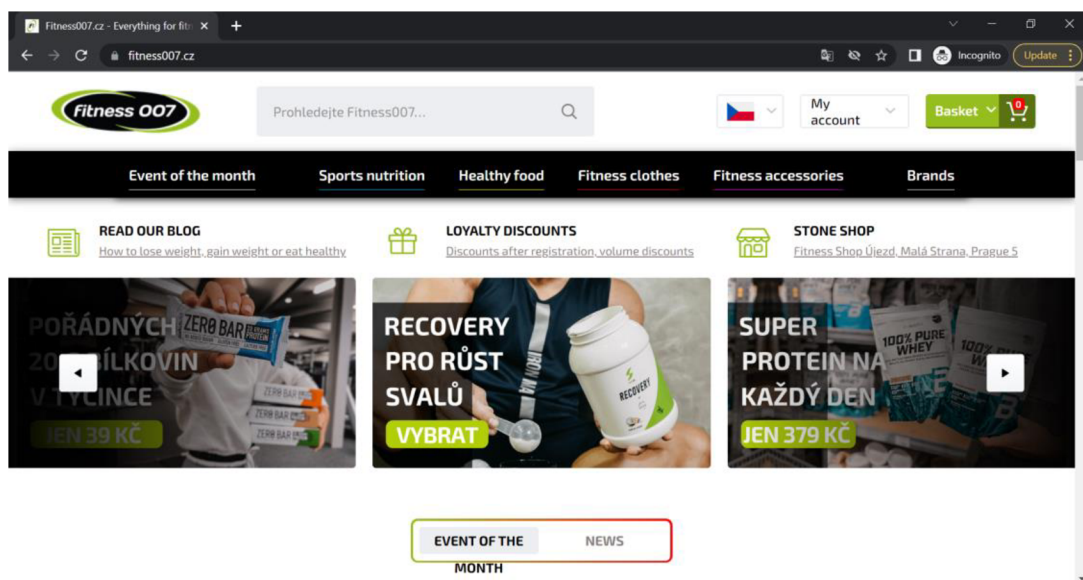


Source: www.fitness007.cz

However, under the GDPR, websites need to obtain proper user consent before

collecting and processing personal data using cookies. A cookie banner or pop-up that explains how cookies are used and gives users the choice to accept or reject the usage of cookies is typically how this is accomplished. However, the website being discussed doesn't have a cookie banner or any option for users to allow or reject the processing of their data when they land on its home page (figure 2). Therefore, it does not comply with GDPR requirements for cookie consent and data collection. To comply with GDPR laws, the website needs to provide users a banner or pop-up displaying cookies. This allows for consent options regarding data collection and ensures adherence to regulations set forth by GDPR.

Figure 2 Home page of fitness007.cz



Source: www.fitness007.cz

2. Does the website have a privacy policy that is easily accessible, and does it clearly state the type of personal data being collected, the purpose for which it is collected, and how it is processed?

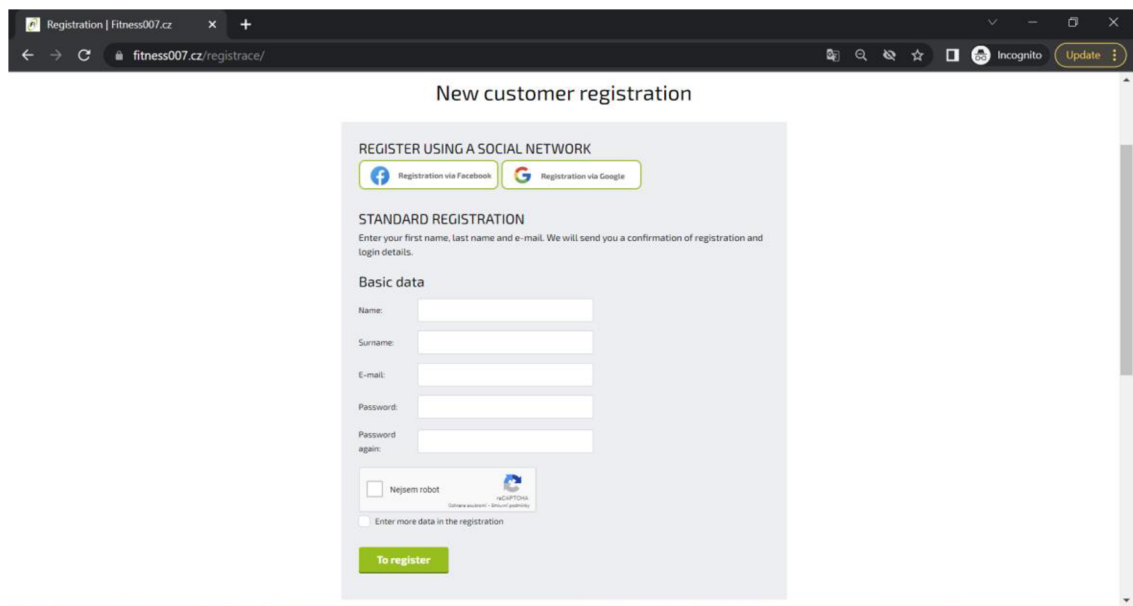
There exists a privacy policy on the website which can be easily located. The footer of the website contains a link for accessing said policy, but it is also available while registering.

The policy on confidentiality explicitly lists the classifications of private information that are gathered, which is personal names, e-mail addresses, telephone numbers and

address. The prime objective for collecting such data is also straightforwardly disclosed; to offer services provided by the website itself as well as processing payments and to interact with users regarding their corresponding profiles (Figure 3). Regarding the handling of information, the policy on confidentiality specifies that any data obtained is dealt with in a manner consistent with its original purpose. The website guarantees users are made aware of both what information is collected and why it's being collected while also granting them the right to disagree should their info be processed under certain conditions. Additionally, measures have been put in place-both technical and organizational-to safeguard private details against illegal or unauthorized manipulation.

As a whole, the privacy policy found on <https://www.fitness007.cz/> seems to fully satisfy all of the stipulated GDPR standards as they adhere to openness and comprehensibility with regard to gathering, handling, and retaining individuals' private data.

Figure 3 Sign Up Page



The screenshot shows a web browser window with the URL fitness007.cz/register/. The page title is "New customer registration". It features two main registration paths: "REGISTER USING A SOCIAL NETWORK" with buttons for Facebook and Google, and "STANDARD REGISTRATION". The standard registration form includes a heading "STANDARD REGISTRATION" with a sub-heading "Basic data" and several input fields: "Name:", "Surname:", "E-mail:", "Password:", and "Password again:". Below the form are two checkboxes: "Nejem robot" (with a reCAPTCHA logo) and "Enter more data in the registration". A green "To register" button is positioned at the bottom of the form.

- 3. Does the website provide users with a way to exercise their rights under GDPR, such as the right to access, rectify, and delete personal data?**

The policy says that the users have the right to request access to their personal data, the correction of any errors, and the deletion of their personal records, as stated in the website's confidentiality policy. The administrator shall provide a maximum of one month for the necessary actions to be done after receiving such requests as expressly mentioned in this document.

Nevertheless, these clauses do not specify specific procedures for implementing the aforementioned rights.

4. Is there a clear and efficient process in place for users to submit requests related to their personal data?

It's uncertain whether users have access to a streamlined process for submitting personal data requests. Despite the website's privacy policy outlining user rights and measures they can take; it FAILS in offering explicit instructions or a straightforward procedure for making those requests.

5. Does the website provide proper security measures, such as encryption and firewalls, to safeguard personal data?

The security protocols implemented by the website to ensure protection of personal data cannot be readily ascertained.

Despite the assertion in the website's privacy policy about its implementation of measures for protecting personal data, there is a noticeable shortage when it comes to elaborate explanations of these methods. There are several procedures that could be employed here such as encryption and firewalls among others but unfortunately, they have not been explained adequately enough.

Devoid of said crucial element, evaluating and gauging the efficacy of a website's protective measures against unwarranted entry, divulgement, manipulation or maltreatment of private and delicate personal information would prove quite arduous.

6. Are there procedures in place to detect and report data breaches, and how are data breaches handled?

The website's capability to securely store personal information is uncertain. The privacy policy includes security protocols but fails to elaborate on the type of

technology used - for example, firewalls or encryption methods. This lack of explanation contributes to further ambiguity regarding data protection practices. Lacking such crucial details, it is difficult to assess the effectiveness of the security measures used by the website to protect personal data from unauthorized access, disclosure, or misuse.

7. Are there data protection officers or data controllers responsible for monitoring GDPR compliance, and is their contact information available on the website?

The matter of who specifically is accountable for ensuring compliance with GDPR and whether their contact details are readily accessible on the website remains obscure at present.

The website's privacy statement does not provide any particular information on the people or organizations in charge of GDPR compliance, nor does it include any contact details for data protection officers or data controllers.

8. Are there any third-party providers that the website shares personal data with, and if so, is their GDPR compliance verified?

Yes, based on the information provided, the website shares personal data with two third-party providers, Heureka and Zboží.cz, for the purpose of recording purchase conversions and email addresses. Additionally, the website shares personal data with Sklik for the purpose of recording cookies, website usage, and purchase conversions. While the website does not explicitly state whether their GDPR compliance has been verified, they do mention that Heureka is the operator of the Heureka.cz portal, and they provide a link to the Conditions of the Verified by customers program. This suggests that Heureka is a reputable third-party provider that is likely GDPR-compliant. However, it is unclear whether Zboží.cz and Sklik are GDPR-compliant, as the website does not provide any information on their compliance status.

9. Does the website comply with GDPR requirements in its email marketing practices, including opt-in consent, and the ability for users to unsubscribe or withdraw their consent?

It appears that the website complies with GDPR requirements in its email marketing practices. The website states that it will only send commercial communications to users who have not refused such communication in accordance with Section 7, Paragraph 3 of the Act on Certain Information Society Services (No. 480/2004 Coll.). This suggests that the website is seeking opt-in consent from users before sending them commercial communications. Additionally, the website provides a clear and easy-to-use mechanism for users to unsubscribe from commercial communications. Users can do so by clicking on the "Unsubscribe" link included in every email communication sent by the website. Overall, it seems that the website has implemented measures to ensure that it complies with GDPR requirements regarding email marketing practices.

4.4. Risk Assessment

This section of the thesis spots the risk possessed with non-compliance to GDPR and provides rating using risk matrix.

We will utilize a risk matrix, which takes the possibility and effect of a risk occurring into account, to complete a quantitative risk assessment. The probability of a risk materializing can determine the level of likelihood which may be graded as low, medium or high. Based on how severe the repercussions are if such risks become reality, the impact is evaluated and scored accordingly from low to medium or high levels.

Here is the risk matrix that we will be using:

Likelihood/Impact	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	9

Using the information provided, here are the risks and their likelihood and impact:

1. Risk of unauthorized access and misuse of personal data due to the volume and type of data collected:

Likelihood: Medium

Impact: High

This risk is medium in likelihood and high in impact, as the large volume and sensitive nature of personal data collected makes it an attractive target for unauthorized access and misuse. The potential impact of a data breach could be significant in terms of financial loss, damage to reputation, and loss of customer trust.

Risk rating: 6

2. Risk of identity theft and financial fraud due to the sensitivity of the personal data collected, particularly billing information:

Likelihood: Medium

Impact: High

This risk is of medium likelihood and high impact, as billing information is particularly sensitive and can be used for fraudulent activities if compromised. The potential impact of a data breach could be significant in terms of financial loss, damage to reputation, and loss of customer trust.

Risk rating: 6

3. Risk of data breaches and unauthorized access due to unclear security measures:

Likelihood: High

Impact: High

This risk is high in likelihood and high in impact, as unclear security measures may leave the personal data vulnerable to unauthorized access and misuse. The potential impact of a data breach could be significant in terms of financial loss, damage to reputation, and loss of customer trust.

Risk rating: 9

4. Risk of improper handling of data breaches and data subject access requests due to unclear procedures:

Likelihood: Medium

Impact: Medium

This risk is of medium likelihood and impact, as unclear procedures may lead to improper handling of data breaches and data subject access requests. The potential impact of improper handling could be significant in terms of financial loss, damage to reputation, and loss of customer trust.

Risk rating: 4

5. Risk of non-compliance with GDPR regulations by third-party data

processors:

Likelihood: Medium

Impact: High

This risk is of medium likelihood and high impact, as non-compliance with GDPR regulations by third-party data processors may result in fines and loss of customer trust. The potential impact on the organization could be significant in terms of financial loss and damage to reputation.

Risk rating: 6

6. Risk of inadequate user consent mechanisms, potentially leading to non-compliance with GDPR regulations:

Likelihood: High

Impact: High

This risk is of high likelihood and impact, as inadequate user consent mechanisms may lead to non-compliance with GDPR regulations. The potential impact on the organization could be significant in terms of monetary loss and damage to reputation.

Risk rating: 9

7. Risk of non-compliance with GDPR regulations and loss of user trust if the procedures for exercising data subject rights are unclear or difficult to follow:

Likelihood: Medium

Impact: Medium

This risk is of medium likelihood and impact, as non-compliance with GDPR regulations and unclear procedures for exercising data subject rights may lead to

loss of user trust. The potential impact on the organization could be significant in terms of monetary loss and damage to reputation.

Risk rating: 4

8. Risk of user frustration and dissatisfaction if the process for submitting requests related to personal data is unclear or inefficient:

Likelihood: Medium

Impact: Low

This risk is of medium likelihood and low impact, as unclear or inefficient processes for submitting requests related to personal data may lead to user frustration and dissatisfaction, but are unlikely to have a significant impact on the organization.

Risk rating: 2

Risks with a risk matrix score of six or above are deemed high-risk and demand quick action. Hazards with a grade of 3-5 are considered to be medium-risk and need attention.

As a result, risks 1, 2, 3, and 5 and 6 should be addressed right once, and risks 7 and 4 should also be addressed to lessen the possibility of their happening.

5. Results & Discussion

The GDPR regulations are not fully followed in certain areas of the e-commerce website. Personal data such as names, email addresses, phone numbers and billing information is collected without any clear indication regarding safety precautions taken to protect this sensitive personal data. Moreover, it remains ambiguous whether there are efficient procedures for detecting or reporting potential breaches related to user's private details on the site. The third-party providers with whom customer information is shared can also be non-GDPR compliant which can result in further security issues. Though an explanation documenting cookie usage and consent gathering processes exists within the platform; a banner warning visitors about cookies or granting users permission when they enter isn't available yet. Users do have access to clarification

around their rights under GDPR but how these individuals could exercise those rights was obscurely put forth. The overall improvement required pertains towards establishing explicit instructions that allow effective functioning vis-à-vis processing privacy requests keeping seven principles of GDPR at its core. To summarize, this situation calls for heightened security measures along with transparent service provisions highlighting precisely defined protocols that assist customers while exercising their legal right over personal records. Below is an analysis of how this information can be presented in terms of the seven principles of GDPR:

- I. In terms of the first principle of GDPR which is principle of Lawfulness, Fairness, and Transparency, the website's privacy policy clearly states the type and purpose of personal data being collected and processed, promoting transparency.
- II. The website collects only the necessary personal data required to fulfil its purposes, recognizing the level of sensitivity of the personal data being collected as per the principle of Data Minimization
- III. The website strives to maintain its commitment towards the principles of Integrity and Confidentiality. It states that user privacy is safeguarded through various measures put in place, however, it doesn't reveal the details of specific procedures employed for confidentiality purposes.
- IV. According to principle of Rights of the Data Subject, users have the right to view, update, and delete their personal information in line with a website's privacy policies. Even though these policies exist, they are deficient in providing guidelines on how one can practically execute such rights promptly.
- V. The website exchanges user information with third-party providers for particular reasons in accordance with Principle of Controller and Processor Responsibility, although it is not obvious if these providers are GDPR compliant.

- VI. The website provides a clear explanation of how it obtains valid consent for data collection, but it does not have a cookie banner or any option for users to allow or reject the processing of their data when they land on its home page.
- VII. For users to submit requests specific to their personal data, a clear and quick procedure must be developed in order to maintain the Principle of Accountability. However, it appears that there is uncertainty on whether such a system is used.

5.1. Recommendations

The thesis aimed to provide the website with best practice compliance recommendations as a secondary objective. The following are the recommendations suggested:

1. Examine and revise the privacy policy to authenticate that it includes additional particulars on the protective actions exercised to maintain personal data. It is crucial that an explicit portrayal of distinct security measures employed are present in this document.
2. Create and put into action protocols for identifying and notifying data breaches. Establishing clear methods for handling and reporting data breaches to the right regulating agencies, together with thorough guidelines describing the proper course of action, is essential.
3. Implement a cookie banner or similar facility to obtain valid consent for data collection on opening the website link. The user has to accept or reject the processing of their data.
4. Develop a clear and efficient process for users to submit requests related to their personal data. The website should ensure that the procedural guidelines outlined encompass detailed directions on how consumers may exercise their GDPR rights, comprising but not limited to accessing, rectifying and erasing personal information. Conduct due diligence on third-party data processors, such as

Heureka, Zboží.cz, and Sklik, to ensure they are GDPR-compliant. If they are not, the website should consider finding alternative data processors.

5. Train employees on GDPR compliance and ensure that they understand the policies and procedures in place for handling personal data.
6. Conduct regular reviews of the website's data processing practices and update policies and procedures as necessary to ensure continued GDPR compliance.

5.2. Limitations

Limitations in conducting a compliance check on an E-commerce website, especially when it is done without the involvement of the website owner include:

- **Limited scope:** A compliance check conducted without the website owner's involvement may be limited in scope, focusing only on publicly available information. This may not provide a comprehensive understanding of the website's compliance status.
- **Access restrictions:** Some aspects of compliance, such as security measures or data handling processes, may require direct access to the website's systems or records. Such access might not be possible without the website owner's awareness.
- **Being unable to recognize every possible compliance issue:** The difficulty in identifying every potential compliance issue or risk related to a website's data protection practices: Without the owner's active participation, it is impossible to identify every potential compliance issue or risk.
- **Access to internal policies and procedures is restricted:** If the owner is not actively involved, accessing the website's internal policies and procedures relating to data protection, security measures, and data processing processes is difficult. Due to severe accessibility restrictions, getting copies of this information seems unachievable.
- **Verification of data authenticity cannot be guaranteed:** Establishing the truthfulness of provided details can prove to be a daunting task. The accuracy,

relevance, and applicability of the information on this specific website might not hold up. Validating every piece of information becomes a difficult task without the controller's assistance.

6. Conclusion

The findings of this thesis emphasize the significance of complying with GDPR regulations for e-commerce platforms. With data privacy and security being top priorities for consumers, it is essential for businesses to handle personal data transparently and securely. In the case of fitness007.cz, there are areas where the website could improve its compliance with GDPR requirements despite having some measures in place to protect users' data and acquire consent.

One way that fitness007.cz could improve its compliance is by enhancing its security measures to safeguard sensitive personal data. Moreover, greater transparency around the handling of personal data and sharing with third-party providers would enable users to make informed choices about their data privacy. Additionally, providing clear instructions on how to exercise GDPR rights such as the right to access, rectify, and erase personal data would empower users to take control of their data.

The importance of GDPR compliance in the e-commerce sector is emphasized in this thesis' conclusion, the fitness007.cz's GDPR compliance level is evidently Medium Low. This study seeks to assist the website in reaching optimal compliance practices and proving its dedication to user data privacy and security by finding areas of non-compliance and offering suggestions for improvement.

7. References

1. European Union. (2016). General Data Protection Regulation. Official Journal of the European Union: Luxembourg: Publications Office of the European Union, 59. ISBN 978-92-79-46107-4.
2. Marelli, G. (2018). A Brief History of Data Protection Law. In Data Protection and Privacy (pp. 1-18). Springer. https://doi.org/10.1007/978-3-319-92928-4_1
3. Witzleb, N., Lindsay, D., & Paterson, M. (2019). Principles of Data Protection in Europe: Challenges and Opportunities. Oxford University Press
4. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council, commonly known as the General Data Protection Regulation (GDPR) . <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
5. EU Commission. (2021). Guidelines 06/2021 on the application of Article 65(1)(a) GDPR Version 1.0. ISBN 978-92-76-35282-5
6. International Association of Privacy Professionals (IAPP). GDPR Text: Regulation (EU) 2016/679 [PDF]. 2016. <https://iapp.org/media/pdf/library/Europe/Regulation/EUGDPR-Language-Versions.pdf>
7. The Office for Personal Data Protection. GDPR (General Regulation) [online]. Version unspecified. Prague: The Office for Personal Data Protection. [cited 2023 Mar 9]. <https://www.uoou.cz/gdpr-obecne-narizeni/ds3938/p1=3938>.
8. The Office for Personal Data Protection. Rights of the Data Subject [online]. Version unspecified. Prague: The Office for Personal Data Protection. [cited 2023 Mar 9]. <https://www.uoou.cz/6-prava-subjektu-udaj/d-27276>.
9. ICO. (2020). Guide to the General Data Protection Regulation (GDPR). Rights related to automated decision making. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>
10. GDPR. Transfer of personal Data to third party countries or international organization [online]. Publication/version. EU GDPR]. <https://gdpr.eu/transfer-of-personal-data-to-third-countries/>
11. GDPR. European Data Protection Board [online]. Publication/version. EU GDPR, <https://gdpr.eu/european-data-protection-board/>

12. ICO. Independent Supervisory Authorities. [online] Publication/version. Place of publication: Information Commissioner's Office, 2021
<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/independent-supervisory-authorities/>
13. IT Governance Publishing. EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guide. 1st edition. 2017. ISBN 978-1-84928-982-9
14. Watkins, S. G. ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. 2nd edition. 2016. ISBN 978-1-84928-714-6
15. European Data Protection Board (EDPB). Guidelines 03/2019 on the processing of personal data through video devices [PDF]. 2019.
https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-032019-processing-personal-data-through-video_en
16. O'Connor, E. (2018). GDPR: what you need to know. [Online]. UK: ComputerWeekly.com.
<https://www.computerweekly.com/feature/GDPR-What-you-need-to-know>
17. Kuner, C. (2020). The EU General Data Protection Regulation (GDPR): A Practical Guide. Oxford University Press. ISBN: 9780198826491.
18. Dinev, T. & Hart, P. (2021). Privacy and security concerns in e-commerce. In E-Commerce Security and Privacy: Protecting Intellectual Property and Consumer Rights (pp. 27-54). Springer. ISBN: 978-3-030-81168-4.
19. Kpmg. (2017). GDPR readiness: Key challenges for online businesses. Retrieved from
<https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/05/gdpr-readiness-online-businesses.pdf>
20. Garvey, B. (2018). How to prepare for GDPR in e-commerce. Website Magazine, 24(5), 28-30. Retrieved from <https://www.websitemagazine.com/blog/how-to-prepare-for-gdpr-in-e-commerce>

