Asta Petrosiute

Ensuring Data Privacy Through GDPR in a Large Organization

A Case Study

Metropolia University of Applied Sciences

Bachelor`s Degree

Degree Programme in Information Technology

Thesis

17.06.2025

Abstract

Author(s):	Asta Petrosiute
Title:	Ensuring Data Privacy Through GDPR in a Large Organization
Number of Pages:	31 pages
Date:	17 June 2025
Degree:	Bachelor`s degree
Degree Programme:	Degree Programme in Information Technology
Specialisation option:	
Instructor(s):	Janne Salonen (Advisor)

Data privacy and data protection has become a very frequent subject of discussion in today`s digital era. Because of the anticipated increase in privacy incidents and data breaches regulators worldwide are implementing stricter measures like the General Data Protection Regulation (GDPR) of the European Union. The regulation is promoting important data protection safeguards and brings not only new challenges, but also potential opportunities to organizations around the world, and a lot of organizations are not yet properly ready for compliance with the GDPR.

This thesis examines how large companies implement GDPR compliance in practice. The study applies a qualitative methodology that combines case study and content analysis. GDPR principles are used to code and analyze Philips' privacy documents and website content. Through theoretical perspective, relevant insights on the topic were gained and knowledge base has been created. The study backs its aims by bridging theory with real world practice.

Results show that the case study company demonstrates strong GDPR compliance by applying clear privacy communication, structured data governance as well as robust data security practices. The company informs users in an effective way of their rights and legal grounds for data processing. On the other hand, breach notification protocols and data retention transparency areas could be improved. To conclude, the company in question could be used as a model for GDPR implementation in large international businesses, but findings may not be directly generalizable to all organizations.

Keywords: General Data Protection Regulation (GDPR), privacy, data privacy, personal data

---

Contents

1 Introduction and Aims of the Thesis

As technology, including ICT, advances, there is a growing need for data about people, and it is considered an important asset for organizations, governments and other entities. Not only big data is useful and applicable to many fields, but there is also emergence of digital platforms, cloud computing, social media and new technologies like machine learning, artificial intelligence (AI) and the Internet of Things (IoT) data that also have become valuable resources for businesses. Companies due to engaging in competition need to engage in customer surveillance to collect market intelligence. More and more of modern economic activity, innovation, and growth cannot happen without data (Mira, 2023) which brings a vast amount of possibilities.

Concerns regarding people`s right to privacy and the security of personal data however have also grown as a result of this enormous data collection and use. And notions of privacy makes it difficult to keep up with technology advancements, the development of technology cannot meet the immediate demand for privacy protection (Sun et al., 2021).

It is also noticeable that there is augmentation of risks associated with the privacy of the individual beings whose data are being collected and analysed, and which often is happening without them being aware of it (Soria-Comas & Domingo-Ferrer, 2015). So often, person's knowledge or consent can be missing. But numerous consumers voluntarily divulge their personal data in return for advantages like location-relevant mobile content as well as enhanced convenience and customized online offers. And there is a growing number of clients voicing concerns regarding their privacy (Okazaki et al., 2020).

The topic of data privacy and data protection has become very frequent in policy debates. As a result of the anticipated increase in privacy incidents and data breaches regulators worldwide are implementing stricter measures like the

General Data Protection Regulation (GDPR) of the European Union (Okazaki, 2020). The EU's GDPR is pushing for important data protection safeguards and brings not only new challenges, but also potential opportunities to organizations around the world, and a lot of organizations are not yet properly ready for compliance with the GDPR (Li et al., 2019).
In this study I aim to investigate how large companies implement data privacy via General Data Protection Regulation in the real world business context.

1.1 Presentation of the subject and the perspective, reasons for choosing the subject

I will focus on how companies implement GDPR to ensure data privacy. I have chosen this topic because, from the business perspective, data occupies a central part in the business context, and data handling that they perform impacts every individual`s personal data, but it can also have implications on the business itself.

Regulations like GDPR has more and more impact on business practices, and it is of importance to see how this regulation is applied in real word business practice. So, it is worth delving into. A thorough examination will be performed to connect insights from theory with practical application in regard to data privacy through GDPR application in the business context of large organizations.

1.2 Definition of the research question or problem

The specific research objectives are:

- To create a theoretical foundation by analyzing the fundamental concepts of data privacy and GDPR to support the analysis of GDPR implementation in the business practice.
- To examine how large companies implement GDPR compliance measures within their data handling practices.

- To explore how large companies communicate their data privacy policies to users through their website.

Here the interest especially falls on international organizations that operate globally with its business operations in the European Union (the Netherlands).

The related research questions would be the following:

- How do large organizations implement compliance with GDPR via their website privacy policies and data handling practices?
- What measures do large companies apply to inform users of their data protection rights and to make sure their personal data under GDPR is safeguarded?

There is a limited number of research questions due to the limited scope of the Bachelor thesis, but my goal was to make them as specific as possible.

When I formulated my research questions, I have thought about what methods would help me to get answers to my questions. And based on the research question, I have chosen the most appropriate research method which will be further discussed in the Research Methodology section.

2 Knowledge Base or Theoretic Starting Points

2.1 Definition of the Key Concepts in the Work Based on Source Literature

To start to understand data privacy and its related concepts as well as EU GDPR law concepts, we need to first understand what is privacy itself and why it is worth protecting. Then data privacy and its different concepts as well as GDRP concepts will be presented.

Privacy

There are numerous distinct definitions of privacy. It can be separated to the ability to prevent intrusion in person's physical space ("physical privacy", for

instance, with regard to the protection of the private home) and to the ability to control the collection and sharing of information about oneself ("informational privacy") (European Data Protection Supervisor (EDPS), n.d.). Privacy can be viewed as a range that represents the various degrees of intimacy and trust with various people. Additionally the definition and expectations of privacy vary among individuals and groups (Markkula Center for Applied Ethics at Santa Clara University, 2013).

Privacy can be put to two types of levels: first is implied or unspoken rules and the second is written legislation. Implicit rules include behaviors, norms, and values about confidentiality that people understand but do not automatically reveal (Knight, 2024). To understand privacy more widely, as noted by Solove (2015), we can view it as an actual product of norms, activities as well as legal protection.

It can also mean respecting the desires of every individual compatible with the aims of the larger community. It is also hardly an individual right, but it can also be considered as a crucial part of any thriving community because it allows people to break away from the encroaching of the community (Solove, 2015). It is about protection from information gathering by others (Tavani & Moor, 2001), not only that it is about notions of being kep away from public, but also notions of withdrawal, seclusion, secrecy (Donaldson, & Lohr, 2020).

Privacy concept can be understood as freedom from not authorized intrusion and the quality or state of being separate from company or observation (Merriam Webster, 2020). It can also be defined as the right to be let alone, or freedom from interference or intrusion (Privacy Professionals (IAPP), 2020). Privacy right is right to enjoy access and using it by oneself (Clayton et al., 2019).
Although privacy is still a human right in the digital age our everyday digital lives and the seemingly endless amounts of data we generate imply that privacy is a commonplace distributed and technologically mediated concept (Gstrein &

Anne Beaulieu, 2022). Despite of different existing definitions and discussions about it, current privacy laws do not offer as much privacy as many people expect or mistakenly believe they have regardless of how one defines privacy (Clayton et al., 2019).

Datafication

Datafication is the process collection, processing, storage and circulation of data which are central elements of a large number of sectors of contemporary societies (Cieslik & Margócsy, 2022). Despite its potential to promote creativity economic growth and well-informed decision-making the datafication process still presents significant challenges. Data privacy concerns security flaws ethical considerations and regulatory complications are just a few of the challenges (Singh et al., 2024).

Data Privacy

Data privacy can be understood as the rules through various laws and regulations to personal data about people that organizations collect, store, use and disclose (Data Protection, 2022); it is a set of certain principles and guidelines to make sure there is respectful processing, protection, as well as handling of sensitive data linked to a person (Knight, 2024). So, data privacy is the principle that individuals should have control over their personal data which actually includes the ability to decide how companies collect, store and use their data (IBM, 2023); it is the wish of an individual to control or influence information about them (Ching et al., 2018).

General Organization for Economic Co-operation and Development (OECD) data privacy principles contain: maintaining a high data quality, restricting general data collection, gathering data only for a specific purpose, utilizing data only for a specific aim, applying security guards on sensitive data, holding information about sensitive data processes as open and clear, permitting

persons to dispute data accuracy related to them as well as making companies responsible for following these guidelines (Knight, 2024).

Data privacy is sometimes also called information privacy (Kim et al., 2023; IBM, 2023). It is an individual's aim to control the terms under which personal information which is information identifiable with the individual, and which is acquired, disclosed, and used (Kim et al., 2023); a consumer’s right to take control of the access to, use, and sharing of their personal data (Westin, 1967, cited in Quach et al. 2022).

Information privacy can be understood as an person’s ability to decide the volume and mode of access to information about their personal life (Vitalii, 2021). The author suggests that the narrow understanding of information privacy concerns only the informational aspect, and other parts such as physical, visual, phonetic privacy, etc. are more understood to relate to the content of other fundamental rights. On the other hand, the first understanding is more about information privacy as the right of the person to control their personal data, whereas the second one is about more rational and efficient consideration of information pricing as the right of ownership of personal data (Vitalii, 2021).

Data Protection

According to National Institute of Standards and Technology (NIST) data protection is ”a condition that safeguards human autonomy and dignity through various means, including confidentiality, predictability, manageability, and disassociability” (NIST, n.d.). security strategies and processes that aid in protecting sensitive data against corruption, compromise, and loss, where threats to sensitive data contain data breaches and data loss incidents (Microsoft, n.d.).

Data availability and management are the two main principles of data protection. Data availability makes it possible for employees to obtain the information they require for daily tasks. Sustaining data availability supports company`s disaster recovery and business continuity plan which is a crucial component of data protection strategy, but it depends on backup copies kept in a different location. Having access to these copies helps staff stay productive and reduce downtime. Information lifecycle management and data lifecycle management are both included in data (Microsoft, n.d.).
The goal of data protection is actually to safeguard data and ensure its availability and compliance with regulatory requirements (IBM, 2024).

Data privacy versus data protection and data privacy versus data security

Data privacy and data protection are not the same, they are different terms (Seadle and Havelka, 2023; Hoofnagle et al., 2019). However, they indicate that there is an ongoing debate of which of the two terms is the broader and if and where they crisscross. Other sources indicate that data protection is about maintaining data safe from unauthorized access, while data privacy is about empowering users to take their own decisions about who can handle their data and for what purpose (GDRP.EU, n.d.); privacy maintains the private life whereas data protection assesses whether data is used fairly and with due process (Hoofnagle et al., 2019); these concepts overlap, but do not coincide, the concept of data protection is not the same as concept of data privacy (EDPS, n.d.).

Not only that data privacy and data security are distinct but related disciplines, but both are considered main components of a company's wider data governance strategy (Badman & Kosinski, 2023). Although security is crucial for safeguarding data, it is not enough for dealing with privacy (IAPP, n.d.).

Data privacy principles and human rights perspectives as theoretical basis gave rise to EU General Data Protection Regulation which will be discuss in the chapters that will follow in this thesis.

GDPR Background

According to GDPR Summary, privacy and data protection act as crucial components for a democracy that is sustainable. The GDPR is designed to protect these prerequisites and is an upgrade of the previous EU data protection law (GDPR Summary, n.d.), it replaced the 1995 Data Protection Directive which was adopted. GDPR, as a tool addressing data privacy concerns, has become a global model for data privacy laws in other areas and is regarded as the most stringent data protection law in the world (Schäfer et al., 2023).

The GDPR presses for interacting with personal data via careful planning. It has been established to put in harmony the protection of fundamental rights and freedoms of persons in respect of processing activities and to ensure the liberal flow of personal data between EU Member States (Buri, 2022). GDPR shapes who can collect which information for which purposes, and who has a say in this (Gstrein & Beaulieu, 2022). For businesses it is a framework to apply to ensure that personal data breaches do not appear.

GDPR Applicability

GDPR law is applicable to EU entities that deal with processing personal data as normal part of their own activities or if a company is not from EU, but gives services or goods or monitors behaviour of people in the European Union (European Commission, n.d.). GDPR requires organizations to get user consent to collect data and “implement appropriate technical and organizational measures” to shield personal data of EU inhabitants (Kaushik & Wang, 2018, cited in Li et al., 2019). The regulation also demands organizations/firms to offer

persons robust privacy rights such as Right to be Forgotten, Right of Access to Data, Right to Data Portability, and Right to Explanation of Automated Decision-Making (Kaushik & Wang, 2018, cited in Li et al., 2019).

GDPR application of the data protection regulation does not depend so much on the size of the company/organisation as on the nature of its activities because if company carries out some activities that highly affect the individuals' rights and freedoms there must be more strict rules as per EU GDPR. Importantly, organizations that employ less than 250 people are not obliged to keep records of their processing activities. However, if the company processes personal data regularly, it poses a threat to individuals' rights and freedoms, or it deals with sensitive data or criminal records (European Commission, n.d.).

GDPR Main Concepts

Below are some of the most important terms of the GDRP (GDPR.EU, n.d.):

Personal data — The basic definition of personal data is any information about an identified or identifiable natural person (data subject).
personal data means any information relating to an identified or identifiable Physical disabilities, in medical records and in an employee's evaluation, the name and the social security number, e-mail addresses and the office phone number of an employee are personal data examples. Pseudonymous data can also be considered personal data if it is easy to identify someone from it.

Data processing — Any action performed on data, be it automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing, etc..

Data subject — The person whose data is processed. These can be customers or site visitors.

Data controller — The person who decides why and how personal data will be processed.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

Natural person (‘data subject’); an identifiable natural person is the person who can be identified, directly or indirectly, e.g. by reference to an identifier such as a name, an identification number, location data, religious beliefs, ethnicity, political stance, web cookies, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (EDPS, n.d.).

Special categorization of data that companies cannot process includes the following concepts (Intersoft Consulting, n.d.):

- racial and ethnic origin
- sexual orientation
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic, biometric or health data except in specific cases (e.g. when you've been given explicit consent or when processing is needed for reasons of substantial public interest, on the basis of EU or national law)
- personal data connected to criminal convictions and offences, but there can be an exception, in case this is authorised by EU or national law

GDPR Principles

The European Commission gives 7principles for personal data processing under the GDPR (European Commission, n.d.):

- lawfulness, fairness and transparency
- purpose limitation

- data minimisation
- storage limitation
- accuracy
- integrity and confidentiality
- accountability

These are the rules that companies and organizations must respect, further there is a short explanation of each.

Fairness towards the individuals whose personal data is being processed must be ensured by processing personal data in a way that is both legal and transparent (also known as lawfulness-conforming to law, fairness and transparency).

When a company or organization collects personal data from individuals it must disclose to them the specific purposes for which the data will be processed. For unclear reasons (also known as purpose limitation) a business or organization cannot merely gather personal information. The organization or company must only gather and use the personal information required to accomplish that goal (also known as data minimization) (European Commission, n.d.).

The business or organization is responsible for making sure that the personal data is current and accurate taking into account the reasons for processing it and updating it if necessary (accuracy). Personal information cannot be used by the company or organization for purposes that are incompatible with its original intent. The business or organization is required to make sure that personal information is kept for as little time as is required for the purposes for which it was gathered (a practice known as storage limitation).

Using the proper technology the business or organization must implement the necessary organizational and technical safeguards to guarantee the security of the personal data including protection against unauthorized or illegal processing

as well as against unintentional loss destruction or damage (also known as integrity and confidentiality) (European Commission, n.d.).

GDPR requirements of data handling to organizations

According to GDPR EU (n.d.), he businesses must make sure that only the bare minimum of personal data is processed. Companies should only retain this information for as long as it is needed. Additionally if this information is deemed sensitive they ought to attempt to encrypt it and/or pseudonymize it.
The process of masking data by substituting artificial identifiers for any identifiable or identifiable information is known as pseudonymization. However pseudonymization is limited even though it can be a great way to protect the security and privacy of personal data. Although a person cannot be directly identified using pseudonymous data it is relatively easy to identify them indirectly (GDPR EU, n.d.).

Encryption and pseudonymization function similarly. By substituting different data for unique identifiers it obfuscates personal information. In contrast to pseudonymization which permits anyone with legitimate access to the data to view a portion of the data set encryption restricts access to the entire data set to authorized users. According to the GDPR encryption and pseudonymization can be applied jointly or independently and many businesses decide to employ both strategies in order to safeguard their data subjects (GDPR EU, n.d.).

One of the new requirements regarding of hiring Data Protection Officer Data Protection Officer applies to all companies, including small and medium organizations, but only if processing is their main business and it brings specific threats to the individuals' rights and freedoms, and especially if there is activity of monitoring of individuals or processing of sensitive data or criminal records or/and it affects many people (done on a large scale) (European Commission, n.d.).

Effects of GDPR on businesses

GDPR has influenced how businesses view privacy as an essential component of their operations rather than merely a responsibility to comply, it motivated corporate culture establishing an ethical and sustainable data ecosystem (Klinton et al., 2024). Companies require to actually put a lot of money and human and other resources on updating their technology platforms, changing privacy policies, updating advertising practices and adapting data storage and processes. Foreign companies such as Chinese and American companies have also had to adapt and to upscale their resources to meet demands of GDPR (Li et al., 2019).

The GDPR became like a data governance framework, it stimulates companies to consider meticulously about data and to come up with a plan for the collection, use, and destruction of the data. The regulation can cause some firms to augment the utilization of data in their activities, particularly if the firms are not data-intensive, then they can realize the usefulness of data. Some companies can also find a chance to more precise evaluate the value of their data, changing the data to an actual strategic resource or advantage, just as patent portfolio or copyrights (Hoofnagle et al., 2019).

Interesting to note that some studies (Blind et al., 2023) found out the regulation of EU GDPR encouraged companies to organize again their data management in a more thorough way than they would have done if there was no GDPR in place, bringing up possibilities for ameliorating their existing products. However, there was also the need for extra resources for complying with the new EU regulation which restrained their capacity for generating completely new products.

GDPR has implications on organizations' cybersecurity policy because it demands companies to apply proper data protection measures to protect consumers' personal data and privacy against data loss or exposure. There is

now a strict GDPR requirement towards the data controller to “notify the personal data breach to the supervisory authority without undue delay and, where possible, within 72 hours after they have become aware of it, this measurement is because many cybersecurity incidents and data breaches happened in the past. This will force organizations to address the problem of deficiency of cybersecurity professionals and data protection officers for their firms (Li et al., 2019).

GDPR most likely will negatively affect new technology development and use increasing increase the cost to develop new technologies. One of such type of technologies is Artificial Intelligence (AI) applications with augmented cost and restricted scope because GDPR demands that certain algorithm decisions be reviewed and explained by human beings) which will most likely augment labour cost (Li et al., 2019).

Consequences if GDRP rules are not met or non-compliance

Companies could lose the trust of consumers because 39% of consumers will spend more when they are convinced that an organization protects their personal data which means obtaining consumer trust thanks to data privacy and security could lead to more sales and lead into competitive advantage (Li et al., 2019).

Not only that GDPR creates both internal and external mechanisms to bolster enforcement efforts, but it has got the attention of the business community because it warns with minimum 8-figure fines (Hoofnagle et al., 2019). So, if companies do not fulfil the requirements set in EU GDPR regulation, they may face large fines from the EU.

2.2 Connecting the Thesis to Previous Knowledge

The purpose of the Knowledge Base chapter was to construct on the existing theoretical research and regulatory information about privacy, data privacy, data protection, other data privacy related concepts, and GDPR contents as well as implications on businesses.

This study does not seek to change or invent new definitions but to apply the defined concepts in the empirical context, and to use it as a conceptual background for the research. They will act as a viewpoint or perspective to help to critically evaluate how they are perceived and applied in the real world-in the company. The GDPR principles especially gives the point of reference assessing the chosen company`s behaviour/activities which will be conveyed in the chapters that will follow.

3 Description of the Implementation of the Thesis/Methodology

This thesis will be qualitative in nature. Qualitative study is for the exploration purpose and is used to generate non- numerical data. As stated by Lim, it is an irreplaceable tool for gathering deep insights and understanding complex phenomena, and gives a unique lens to explore and interpret the complexities of social phenomena. And it helps to find out the “what,” “why,” “when,” “where,” “who,” and “how” behind interactions, rather than only quantifying occurrences. (Lim, 2024).

It is suitable for analysing and understanding of the organizations` activities such as data privacy practices tied to regulator compliance (GDPR). Also qualitative method was employed both for collecting and analysing the material of my study because I want to reach the conclusions based on my study gathered data.

The research questions led to the choice of research method. By application of the method, I aim to give justified and trustworthy responses to the research questions. This thesis adopted qualitative research methods of case study (the *what*) and content analysis (the *how*) to explore in depth how a specific large multinational organization implements GDPR compliance in an actual practice. Case studies bring value by giving contextualized insights into certain issues, and actually facilitating the application of abstract theories to real-world situations (Drew, 2023).

The qualitative method of content analysis is best suited for this thesis as the point of the analysis is to understand communication, to systematically and rigorously delve into its meanings, assumptions, themes, and patterns (Oregon State University, n.d.). Content analysis has been applied for systematical examination and interpretation of textual documents where focus is on GDPR related patterns and themes.

Case Study Company

The case company has been chosen which is Philips. It was chosen based on the relevance to my professional background and due to its significance business operations in the European Union which makes it a subject to GDPR. It is a a large multinational company known worldwide. This company also has a public privacy related content whcih is freely accessible and can be analyzed. Datafication is crucial especially in the Healthcare business where they strive to offer medtech solutions which also entails collecting sensitive personal data.

Data Collection

The privacy information of the case company has been collected mainly from Philips global privacy page available at https://www.philips.com/a-w/privacy.html.

The data has been collected in a systematical way based on sources available openly on Philips website, sources related to data privacy and GDPR. The

documents involved Privacy Notice with a version as of January 2022, Cookie Policy, and Privacy Rules which were downloaded from their website. Also documents related such as privacy contact forms and corporate data privacy principles have been collected. Pages were also saved for archiving from their website related to Philips' data privacy communications and cookie consent mechanisms.

The data collection was done between 8th and 11th of June, 2025 to get the most current documents for this research.

Data Preparation and Analysis

The documents that have been collected were organized into folders by categories such as privacy notices, cookies policy, data protection rules inlcuding controller and processor roles as well as privacy related company statements.

All documents have been read in depth to understand how to build my approach. Key points that were relevant to the thesis research questions have been noted down. Points were related to transparency matters, approaches to personal data handling and user rights communication.

The starting point for each visitor of the company website is the Cookies banner in a pop-up window which provides information about cookies on the webpage. The visual presentation which is a screenshot of it is given in Picture 1 which follows below.

Picture 1. Cookies pop-up (Philips, n.d.)

Development of Coding Structure

The initial coding approach was actually guided by GDPR requirements(e.g. principles) from the knowledge base. The coding foundation was made up of codes as in the example below (Table 1).

Table 1. GDPR based Coding Structure (Author, 2025)

Principle	Code	Description
Lawfulness & Transparency	LAW_TRANS	Statements describing legal basis & transparency
Purpose Limitation	PUR_LIMIT	Statements on purpose of data collection
Data Minimization	DATA_MIN	Text about limiting data collected
Accuracy	ACCU	Text on keeping data accurate

Principle	Code	Description
Storage Limitation	STO_LIM	Text on data retention periods
Security	SEC	Descriptions of data protection measures
Accountability	ACCOUNT	References to Philips responsibility
Data Subject Rights	RIGHT	Communication of user rights and ways to exercise them

Systemic Content Coding

Based on coding structure, relevant parts of documents and website content was coded in a manual way. Each text portion was assigned 1 or 2 codes representing GDPR concept it relates to capture themes. The example of it is provided further.

Table 2. Coding examples from Philips documents and website (Author, 2025)

Extract from Text	**Code**	**Explanation**
"We collect personal data only for specific, explicit, and legitimate purposes." (Philips, n.d.).	PUR_LIMIT	Shows Philips limits data use to clear, lawful purposes
"We ensure that personal data is processed in a transparent manner, providing clear information." (Philips, n.d.)	LAW_TRANS	Philips commits to transparency in data processing
"You have the right to access, correct, or delete your personal data." (Philips, n.d.)	RIGHT	Lists user rights per GDPR

Extract from Text	Code	Explanation
"Data is stored only as long as necessary for the purposes collected." (Philips, n.d.)	STO_LIM	Addresses retention limits
"We apply technical and organizational measures to safeguard data against unauthorized access." (Philips, n.d.)	SEC	Describes security controls Philips uses
"Philips takes full accountability for compliance with data protection laws." (Philips, n.d.)	ACCOUNT	Shows corporate responsibility emphasis
"You can accept all cookies, decline all optional ones, or customize your settings. "Essential cookies are necessary for website functionality and are always active." (Philips, n.d.)	LAW_TRANS	Shows user control options; communicates purpose and necessity
"We process personal data on the basis of your consent, to fulfill a contract with you, or to comply with legal obligations." (Philips, n.d.)	LAW_TRANS	Shows legal basis for data processing

Thematic Analysis

The codes were grouped into relevant themes/patterns after coding to depict how company actually executes GDPR rules.

So, thematic analysis served to group codes into higher categories or so-called themes which will be presented in the Results Chapter.

4 Results

In this Chapter the results are presented from the qualitative content analysis and interpretation of the data from Philips website and data privacy documentation. The interpretation has been done based on GDPR coding structure to identify emerging themes as well as compliance strategies and communication methods. The final outcome was a thematic overview how the company implements GDPR principles and communicates their data privacy policies to users through their website.

After the application of qualitative content analysis, an overview of main themes and interpretation based on system coding was created:

Table 3. Overview of main themes based on system coding (Author, 2025)

Theme	Interpretation
Cookie Consent and Management	The cookie consent option gives users options to accept all, decline all optional cookies, or customize preferences, it follows GDPR's consent requirements. Detailed descriptions are given for each cookie category which improves transparency. This is in line with GDPR requirements requiring informed consent.
Communication of Legal Basis for Processing	The website gives a few legal grounds for processing personal data which concerns consent, contract performance, and legitimate interests.

Theme	Interpretation
	These statements meet GDPR's requirement to inform data subjects of the lawful basis for processing (lawfulness and transparency).
Data Subjects Right Communication and Privacy Notice	There is information about users' privacy rights, including access, correction, deletion, and complaint possibilities. The Privacy Notice forwards to dedicated pages and contact forms that allow using these rights. Privacy notices show why personal data is collected, the aim of processing, data retention time, and how users can use their rights as per GDPR.
Data Security and Breach Management	There is outlined organizational, technical, and physical measures to safeguard personal data. A personal data breach procedure is present, but detailed public disclosure policies on breach notifications were less notified. To identify and minimize potential privacy risks Philips uses Data Protection Impact Assessments (DPIAs).
Data Handling practice	The firm is committed to deleting personal data when no longer necessary, referencing legal obligations and business needs as retention criteria. There are

Theme	Interpretation
	data minimization and purpose limitation highlighted according to GDPR. Specific retention periods are not always detailed, which may limit user clarity. For data transfers and processing ensuring data protection the company adopted Binding Corporate Rules (BCRs)

Final outcome is that the case study shows that Philips has a robust approach to GDPR which it embeds in its operations especially in line with website privacy policy and data handling practice. It applies data protection principles by providing privacy notice, conducting Data Protection Impact Assessments, applying Binding Corporate Rules (BCRs), providing employee privacy training for awareness of data privacy/protection and GDPR principles, applying security measures for personal data protection which it mentions as encryption, security audits and controls of access) as well as employing incident response and breach system.

Communication done through privacy documents and their website shows mostly clearness and detail towards users. There is transparency and accessibility (user-friendly communication) as the privacy communication shows pretty clear language and navigation helped by links and summaries to improve user understanding.

The company gives information to users about GDPR rights (erasure, access, rectification, etc.) via privacy notice, clearly states contact possibilities, not to forget data Protection Officer as well as provides consent over data usage via

withdrawal and controls options. On the other hand there is some complex terminology which may be difficult to understand for all website visitors such as customers.

5 Conclusions and Their Discussion

5.1 Summary of the Key Results and the Conclusions Drawn From Them

Key results revealed how Philips implements GDPR in its operations. Philips employs thorough and lucid GDPR compliance communication, especially on important topics like cookie management, the legal justifications for data processing the rights of data subjects as well as data security measures. In accordance with GDPR regulations Philips website provides good consent options and clearly classifies cookies.

Nonetheless they could improve communication regarding breach notification protocols and more clear disclosure of data retention durations. Overall, Philips demonstrates a high degree of adherence to GDPR when implementing GDPR compliance measures within their data handling practices thanks to a mature and structured approach to GDPR compliance (e.g. GDPR principles) and robust internal privacy governance as well as clear user communication with well documented policies.

5.2 Assessment of How Well the Work’s Aims Were Achieved

The aim of the thesis was to investigate how large companies ensure data privacy via General Data Protection Regulation in the real world context. This was achieved successfully. Thanks to the approach of case study and content analysis, there was a systematic and well researched evaluation of the chosen case study company`s compliance strategy which also provided answers to research questions.

The thesis shows that objectives were fulfilled successfully: data privacy concepts and GDPR concepts were examined through literature and regulatory documents, the examination of GDPR compliance measures within data handling practices in the large companies` business context and user communication strategies has been done using a case study of Philips in combination with content analysis. The analysis was performed based on the company's website and privacy materials.

The findings revealed that Philips meets GDPR compliancy requirements through privacy and cookie policies and data handling practices (cookie consent, purpose limitation, data minimization and storage limitation) and communicates them to users observing transparency, legal bases for data processing, and user rights such as via Privacy Notice and contact forms as well as information to users about data protection.

The thesis aim has been fulfilled both in scope and depth through the combined application of theoretical and practical approaches.

5.3 Reflection on the Work Process and the Results Obtained

The integration of content analysis and case study methodologies showed efficacy in gathering and analyzing pertinent data. A transparent and impartial assessment of Philips communication was made possible by the structured coding framework. There was one difficulty which was interpreting technical and legal terms to actually achieve consistency in coding, but this was resolved by iteratively improving the codes. Coding concentrating on GDPR principles permitted structured analysis as well as thematic consolidation.

5.4 Evaluation of the Ethicality and Reliability of the Work

Regarding research ethics, I did my utmost to conduct my research work in an ethical and compliant manner observing the principles of responsible conduct of research. Since I did not collect material that contains personal data, I did not

take steps to make sure that the data concerning participants in my research are protected.

I put my best effort to include proper in-text citations and references of literature. I sought to use data from diverse sources because it can provide complementary perspectives on the same construct, triangulation due to data sources or collection methods can show evidence of the integrity of the research conclusions. (Coleman et al., 2021).

To show reliability in qualitative study is challenging because it is different from quantitative research, and there are no available statistical tests for this purpose (Coleman et al., 2021). But I have thoroughly considered tools and their application in this thesis to show validity and reliability.

Because in the qualitative study, both validity and reliability are based on trustworthiness, to ensure reliability for this study, I have applied as detailed as possible description of the rationale of research design and implementation to be transparent (Coleman et al., 2021). Audit trial was enabled because I documented steps I took, and decisions made during the study which is one of the strategies of reliability as well (Jarrahi & Newlands, 2024).
I have combined case study approach with content analysis to reinforce reliability of my thesis. Next to framing Philips as a study case, I also systematically analyzed their data privacy practices via their public documents and website content. Also I performed data collection as systematically as possible by actually downloading and archiving certain pages and documents to allow for consistency and reliability.

When doing content analysis through coding and theme identification, the aim was to reduce potential bias during theme identification, for this reflexive approach was employed. The codes and themes that emerged were compared in a continuous way back to the original data and the already defined coding structure was used to reaffirm their relevance and accuracy.

Since the case study approach was employed, the limitation is that results may not be generalizable to all organizations.

5.5 Further Research Possibilities

Further research could involve investigation of efficacy of GDPR or other data privacy policies in practice applying interviews or audits. Comparison of the case study with other multinational corporations could also be done or comparison of multiple companies across different sectors could be done as well. There could also be studies about user perception of privacy policies.

6 References

Badman & Kosinski (2023). IBM: What is data protection? https://www.ibm.com/think/topics/data-protection

Bethlehem, D., Van Damme, I., McRae, D., & Neufeld, R. (Eds.). (2009). The Oxford Handbook of International Trade Law. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199231928.001.000

Blind, K., Niebel, C., & Rammer, C. (2023). The impact of the EU General data protection regulation on product innovation. Industry and Innovation, 31(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858

Ching, M. R. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. Advanced Science Letters, 24(10), 7042–7046. https://doi.org/10.1166/asl.2018.12404

Cieslik, K., & Margócsy, D. (2022). Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data. Progress in Development Studies, 22(4), 352-373. https://doi.org/10.1177/14649934221076580 (Original work published 2022)

Clayton, E. W., Evans, B. J., Hazel, J. W., & Rothstein, M. A. (2019). The law of genetic privacy: applications, implications, and limitations. Journal of law and the biosciences, 6(1), 1–36. https://doi.org/10.1093/jlb/lsz007

Coleman, P. (2022). Validity and Reliability within Qualitative Research for the Caring Sciences. *International Journal of Caring Sciences, 14,* 2041-2045. Pdf

Data Protection." Glossary. International Association of Privacy Professionals. https://iapp.org/resources/glossary/

Donaldson, M. S., & Lohr, K. N. (2020). Confidentiality and Privacy of Personal Data. Nih.gov; National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK236546/

Drew K. (2023). 10 Case Study Advantages and Disadvantages. https://helpfulprofessor.com/case-study-advantages-and-disadvantages/

EDPS (n.d.). Glossary. https://www.edps.europa.eu/data-protection/data-protection/glossary/p_en#privacy

GDPR-EU. A guide to GDPR data privacy requirements. https://gdpr.eu/data-privacy/

GDPR EU. (n.d.).GDPR personal data – what information does this cover?. https://www.gdpreu.org/the-regulation/key-concepts/personal-data/

GDPR Summary, (n.d.). https://www.gdprsummary.com/gdpr-summary/

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1). springer. https://doi.org/10.1007/s13347-022-00497-4

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means*. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

IBM (2023). What is Data Privacy? https://www.ibm.com/think/topics/data-privacy

International Association of Privacy Professionals (IAPP) (2020). What does privacy mean?. The International Association of Privacy Professionals. https://iapp.org/about/what-is-privacy/

Intersoft Consulting (n.d.). Art. 9 GDPR Processing of special categories of personal data. https://gdpr-info.eu/art-9-gdpr/

Jarrahi, M.H., & Newlands, G. (2024). Quality in qualitative research: Through the lens of validity, reliability and generalizability. DOI:10.13140/RG.2.2.21444.23682.

European Commision (n.d.). Data protection explained. https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. Technological Forecasting and Social Change, 196, 122789–122789. https://doi.org/10.1016/j.techfore.2023.122789

Knight M. (2024, April 17). What Is Data Privacy? Definition, Benefits, Use Cases. https://www.dataversity.net/what-is-data-privacy/

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, 22(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Lim, W.M. (2024). What Is Qualitative Research? An Overview and Guidelines. Australasian Marketing Journal, 33(2), 199-229. https://doi.org/10.1177/14413582241264619 (Original work published 2025)

Markkula Center for Applied Ethics at Santa Clara University (2013, February 5). Defining Privacy. https://www.scu.edu/ethics/privacy/defining-privacy/

Merriam Webster (2020). Definition: Privacy. Merriam Webster Inc. https://www.merriam-webster.com/dictionary/privacy

Mira, B. (2023, September 4). Privacy and Data Protection. https://doi.org/10.1093/law/9780192868381.003.0028

NIST (n.d.). Glossary, Data Privacy. https://csrc.nist.gov/glossary/term/data_privacy

Okazaki, S., Eisend, M., Plangger, K., Ruyter, K. de, & Grewal, D. (2020). Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review. Journal of Retailing, 96(4).

Oregon State University (n.d.). Chapter 17. Content Analysis. https://open.oregonstate.education/qualresearchmethods/chapter/chapter-17-content-analysis/

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in Privacy and Data. *Journal of the Academy of Marketing Science*, *50*(1), 1299–1323. Springer. https://doi.org/10.1007/s11747-022-00845-y

Philips (n.d.). Privacy at Philips. https://www.philips.com/a-w/privacy.html

Seadle, M., & Havelka, S. (2023). Information science: Why it is not data science. Data and Information Management, 100027. https://doi.org/10.1016/j.dim.2023.100027

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven Business and Data privacy: Challenges and Measures for Product Companies. Business Horizons, 66(4), 493–504. sciencedirect. https://doi.org/10.1016/j.bushor.2022.10.002

Singh, T., Arvind Panwar, Kuldeep Singh Kaswan, Jain, A., & Urvashi Sugandh. (2024). The Datafication of Everything: Challenges and Opportunities in a Hyperconnected World. Communications in Computer and Information Science, 254–268. https://doi.org/10.1007/978-3-031-58604-0_18

Solove, D. (2015, June 29). What Is Privacy? | TeachPrivacy Privacy Awareness Training. TeachPrivacy. https://teachprivacy.com/what-is-privacy/

Soria-Comas, J., Domingo-Ferrer, J. Big Data Privacy: Challenges to Privacy Principles and Models. Data Sci. Eng. 1, 21–28 (2016). https://doi.org/10.1007/s41019-015-0001-x

Sun, L., Zhang, H., & Fang, C. (2021). Data security governance in the era of big data: status, challenges, and prospects. Data Science and Management, 2, 41–44. https://doi.org/10.1016/j.dsm.2021.06.001

Tavani, H.T. & Moor, J.H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. ACM SIGCAS Computers and Society, vol. 31(1), pp. 6-11.

Vitalii, S. (2021). INFORMATION PRIVACY: A CONCEPTUAL APPROACH. Constitutional and legal academic studies, 52-60. 10.24144/2663-5399.2020.2.06.