**Application of text mining for understanding data protection incidents**

**Nguyen Quang Anh**

Dissertation submitted to International Business School

for the partial fulfillment of the requirement for the degree of

MASTER OF SCIENCE IN IT FOR BUSINESS DATA ANALYTICS

<May, 2025>

**DECLARATION**

This dissertation is a product of my own work and is the result of nothing done in collaboration.

*I consent to International Business School’s free use including/excluding online reproduction, including/excluding electronically, and including/excluding adaptation for teaching and education activities of any whole or part item of this dissertation.*

(Student signature)

Nguyen Quang Anh

Word length: ##,### words

Executive Summary

Table of Contents

[1. Introduction 5](#_Toc196682026)

[2. Literature review 7](#_Toc196682027)

[2.1 Individuals that are protected by the regulation 7](#_Toc196682028)

[2.2 Introducing the general principles of GDPR 7](#_Toc196682029)

[2.3 Summary of related articles 8](#_Toc196682030)

[2.4 Defining data breaches and data protection incidents 8](#_Toc196682031)

[2.5 General knowledge about text mining 8](#_Toc196682032)

[3. Research methodology 9](#_Toc196682033)

[Introducing the Python libraries (Pandas, chosen NLP model, etc.) 9](#_Toc196682034)

[4. Exploratory data analysis 10](#_Toc196682035)

[5. Algorithms and models 11](#_Toc196682036)

[6. Result analysis 12](#_Toc196682037)

[7. Recommendations 13](#_Toc196682038)

[8. Conclusion 14](#_Toc196682039)

[List of references 15](#_Toc196682040)

[Appendix 16](#_Toc196682041)

1. Introduction

Data protection and regulations have been a hot topic in recent years due to the growing expansion of internet users and the rise of social media. As many tech companies are collecting data from their users, the governing authorities had acted to regulate the unlawful collection and processing of personal information. In recent years, the UK and the US banned TikTok from government devices, while India banned the app altogether from the country, citing national security concerns and espionage.

In the European Union, an initiative was started in 2016 called the General Data Protection Regulation, commonly known as the GDPR, to protect people's rights and freedoms. The collection of data privacy laws aimed to harmonize European countries and their data protection authorities, known as DPAs. The ruling became relevant in May 2018 and has been in effect since.

Even though the regulation was released in various forms, due to its difficult legal language and complex connection to different laws and articles, few people know its effects and success. For most internet users, the only noticeable change was a pop-up window asking to opt in to process cookies when browsing, however, the GDPR changed the practices of how companies can collect, store, and process personal data.

The project aims to facilitate the understanding of GDPR and its surrounding laws and definitions for individuals, startups, and small to mid-sized businesses without access to consulting services. As the articles can range from hundreds of words to thousands, it is very time-consuming to read, understand, and apply the rules written. There are estimates that over 90% of people do not read the terms and services conditions before accepting them. Based on this information, we can assume that even fewer people read the regulation on their own.

By utilizing automation software and text mining Python libraries, I am creating an approach to process legal documents and create a list of common mistakes that businesses make. Using the final rulings of penalized businesses for text mining, the expected output is the causes for the incidents, which can be investigated concerning the amount of the fine and the breached article(s). Examining this result can help define the severity of data protection incidents from the perspective of DPAs. If businesses can avoid following the same mistakes that are extracted from the documents, then the likelihood of incidents could drop significantly.

Even though the problem statement focuses more on the business perspective of the regulation, reading the project can also help regular people as well. Understanding our own data protection rights and how companies might misuse data could assist us in taking preventive measures. Knowing what personal data is being collected and what dangers it is exposed to changes our view on the internet and security. Even as an individual we can become data processor by collecting it without knowing. For example, when creating a survey for research or work we can inadvertently collect sensitive information without knowing. Or doing personal projects such as social media scraping for data analysis could be against the rules of GDPR, which is why grasping the concept of it is important.

From a technological standpoint this project introduces a low-cost alternative to existing LLM based text processing. Many businesses cannot afford commercial licenses for these services, therefore a script that can run in a Jupyter notebook should make it accessible. Even though this project focuses processing legal documents, the principles that will be presented can be easily applied to any other text-based research. To be as relevant as possible to the rapidly improving LLM and other text mining models the project will be applying modern text mining techniques where achievable.

However, this collection won’t cover all the possible causes as the rulings are in multiple European languages and due to limitations in time and processing power, only part of them will be added. Articles that haven’t been breached or fined yet also will be missing from the list as there is no input for them. These constraints should be kept in mind when drawing conclusions from the output of this research project.

The scope of the research includes two languages: English and Hungarian. The former is an obvious choice as most text-mining libraries are optimized for this language with many vocabularies. I have included Hungarian as a second language as this is the mother tongue of most of my professors and due to its complexity, it would be interesting to see what results we get compared to English.

The expected outcome of the project is a collection of words and phrases that are connected to the cause of incidents, with exploratory data analysis presenting the legal and technical context surrounding it. The person reading the contents of this paper should get better understanding of European data protection laws while getting a basic level of introduction to data mining methods using Python. The hypothesis is that the vocabulary will include more words and phrases related to unlawful data processing rather than technological or human errors. I believe the regulation is focusing companies with big data, that misuse it by processing it beyond their permitted use. In recent years the same situation happened between Ireland’s Data Protection Commission and, the company behind Facebook, Meta.

The project utilizes prior knowledge and literature from my bachelor’s degree thesis work. However, the technical application and methodology used for the project are different and have no relation to my prior work. During this project I will apply newly acquired skills gained during courses held by IBS. The research method can be considered both primary and secondary as I will be applying libraries and vocabularies prepared by other programmers, but the data collection, preprocessing and conclusion will be my own work.

2. Literature review

To understand where companies can fail data protection inspections, some legal context is needed, which will be briefly explained in the following sections. It is important to know why and how an individual is protected to recognize the breach of one’s rights. After a quick summary of the relevant articles of the GDPR the next section will introduce some of the basic text mining theories in order show the framework the project will be built upon.

## 2.1 Individuals that are protected by the regulation

The first and foremost concept that need to be clarified is which individuals are protected by the articles of the regulation. In law a natural person is defined as a human that can act. make decisions by themselves and legally capable as an individual, distinguishing them from other legal entities such as corporation and organizations. They have fundamental rights such as entering contracts, exercise free speech, privacy and voting. Everyone is entitled to these since birth until their death unless the court of justice restricts them, or the person is not able to act or think independently.

## 2.2 Introducing the general principles of GDPR

In the 5th article of the regulation the general personal data processing principles are established. These are the following:

* lawfulness, fairness and transparency: personal data should be processed in a transparent manner and according to the law
* purpose limitation: data should be collected with a legitimate and specific purpose and should not be used outside this scope. Only archiving for public interest, scientific or historical research are exempt from this limitation.
* data minimisation: only the necessary data should be collected
* accuracy: collected personal data should be accurate and when needed kept up to date, however inaccurate data that is no longer needed should be deleted immediately
* storage limitation: data should be stored in a structure that makes personal data unidentifiable after the processing period ended. Further processing may be permitted in case of achieving purposes mentioned above if appropriate technical and organisational are in place.
* integrity and confidentiality: data should be protected from unauthorised access (data breach), accidental loss (data leak) and unlawful processing (illegal tracking) by using adequate technological and supervisory procedures
* accountability: the data controller must comply with the six principles above and have proof of compliance

## 2.3 Summary of related articles

As the GDPR currently contains 99 articles it would be inefficient to include and explain all of them within this paper. Instead, I will be outlining the more important articles about the rights of the person whose data is collected (data subject) and the obligations towards them in case of a data protection incident.  
  
Every individual has the right to transparent information and communication regarding how their data is processed and where it was obtained. (Art. 12-14) The subject whose data is collected can also request to restrict, erase, object and ask to receive their personal information, to which the data controller/processor can only object to in very limited situations. Not complying to these rights is considered illegal and may incline data subject to make a complaint to the local DPA.  
  
Data processors must notify affected subjects and the local DPA in case of a data protection incident. (Art. 34) The notification should be clear and understandable for the average person and sent immediately as soon as the data breach is discovered. However, the alert can be considered unnecessary by implementing technological and organizational controls that mitigate the effect of the data breach or taking subsequent action to minimize the risk towards the subject. If it would take too many resources for the data processor to inform every individual, then a public announcement should be made with the same effectiveness as direct messaging.

## 2.4 Defining data breaches and data protection incidents

To understand the reasons for regulation and the number of penalties given by DPAs, it is important to know what are threats they are searching for.

A data breach happens when an unauthorized entity gains access to confidential or sensitive data. However, the theft, disclosure, alteration, losing and destruction of protected information is also included in the definition. The cause for data breaches can be both related to technological and human error, which the intruder is exploiting. The most common tactics to gain access include phishing, social engineering, malware and hacking.

Data protection incidents refer to an event where the security or protection of data disrupted. There are many causes for incidents, including data breaches mentioned above, however not all of them result in serious damage if mitigated correctly. For example sending a confidential file and recalling it before the email arrives.

## 2.5 General knowledge about text mining

3. Research methodology

The main objective of the research is to find the most common causes for data protection incidents that were investigated by a supervisory authority and were penalized for insufficient handling of personal data. By employing text mining and natural language processing methods, the expected outcome is a list of words that are present numerous times within these legal documents issued by said authorities.  
  
The main source of data comes from <https://www.enforcementtracker.com/>, which is a website that collects fines and penalties from multiple data protection authorities across Europe. The site tracks the ID of the case (ETid), country, date, the amount of fine, data controller or processor, the article(s) breached, and lastly, the type of issue summarized by the site. As we have access to much of the relevant data extracted already, instead of focusing on extracting this information from the files, I plan to focus on finding the connection between the most common.  
Causes found and the number of fines for articles breached.

While the page hosts many cases from various countries, I will be focusing on documents written in English. As one of the most spoken languages, many Python libraries and vocabularies are built upon it. Of course, the university program is also held in English, which would make it a requirement however, I will be including Hungarian cases as well, either by translating the document or by text mining that is utilizing Hungarian vocabularies.

## Introducing the Python libraries (Pandas, chosen NLP model, etc.)

4. Exploratory data analysis

5. Algorithms and models

6. Result analysis

7. Recommendations

8. Conclusion

List of references

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

Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04> (Accessed: 2025.04.28)

S.1143 - 117th Congress (2021-2022): No TikTok on Government Devices Act Available at: <https://www.congress.gov/bill/117th-congress/senate-bill/1143> (Accessed: 2025.04.28)

Appendix