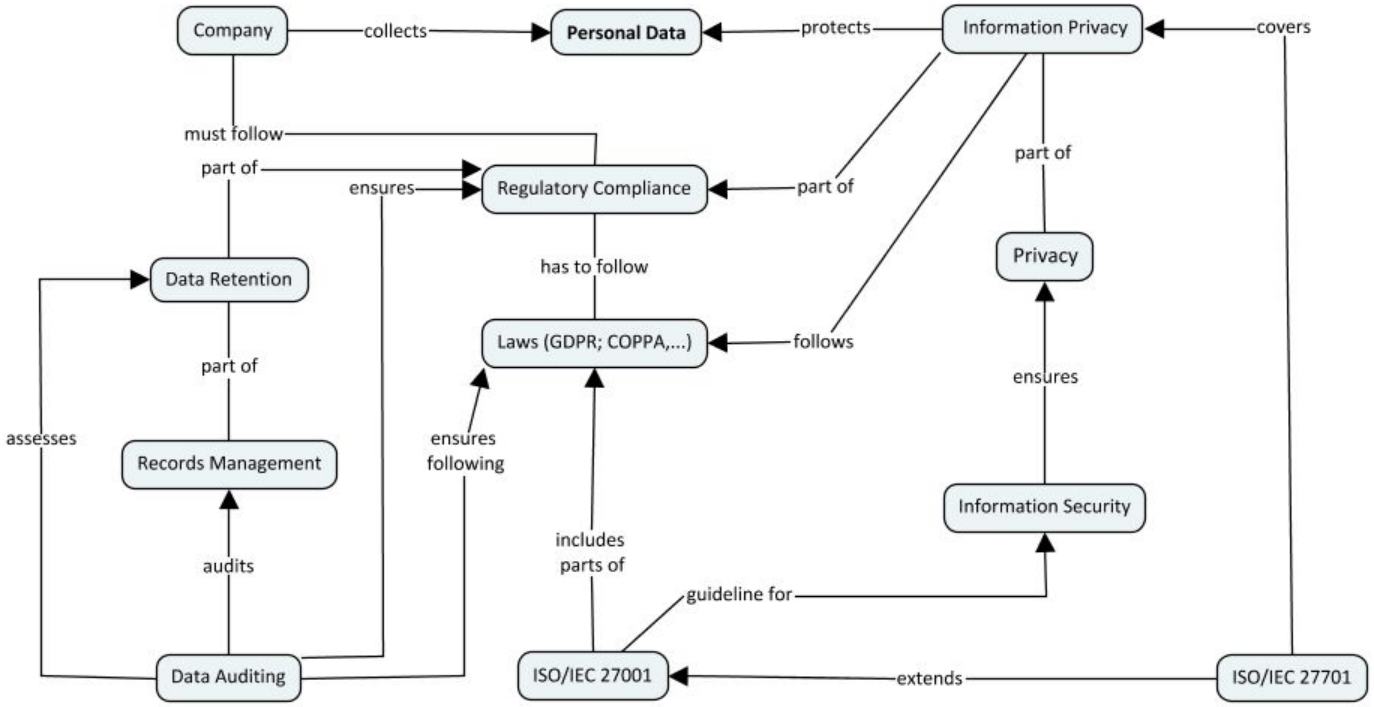
GSI (Case G) - Students numbers (5 digits): 97155 - 97539 - 97540

1 – Conceptual analysis



Concept	Definition (one sentence by concept)
Data Retention	Data retention defines the policies of existing data and records management for meeting legal and business data archival requirements.
Records Management	Records management means, that everything like decisions, sales, data etc. are to be recorded and stored, which is done in an ongoing cycle.
Regulatory Compliance	Regulatory compliance includes laws, policies and regulation, that a company should follow in order to avoid legal consequences.
Privacy	Privacy refers to the non-public area in which a person can exercise his or her right to the free development of his or her personality unhindered by external influences.
Information Privacy	Information privacy includes all laws and is attempting to find the balance between using personal data and ensuring its anonymity.
Personal Data	Personal data is any information relating to an identifiable person.
Information Security	Information security is part of risk management and is about protecting information by analyzing information risks.
Laws (GDPR, COPPA,...)	These laws concern the privacy and data security of people in order to protect their rights as much as possible and to avoid data misuse.
ISO/IEC 27001	ISO/IEC 27001 is an information security standard, that should be implemented by companies.
Company	A company is an economic-financial and legal unit, which is trying to gain as much profit as possible.
ISO/IEC 27701	Standard that is a privacy extension to ISO/IEC 27001
Data auditing	The process of conducting a data audit to assess how company's data is fit for given purpose.

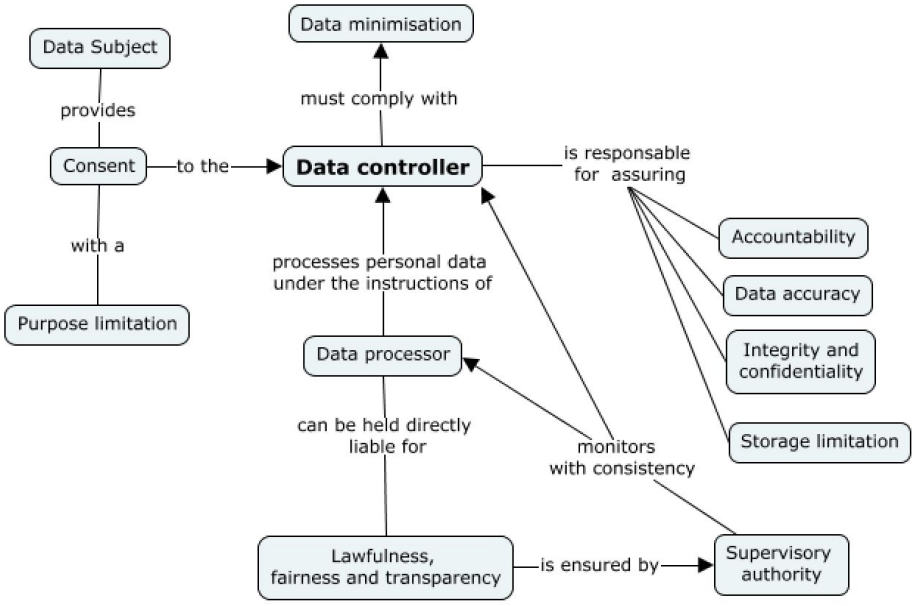
2 – Description of the analysis

With the concept map we try to connect the different concepts within a **company** or organization**.** Every company collects a lot of **personal data,** which gets protected by following **information privacy** rules. The information privacy is a part of **privacy** in general, which means that companies are not allowed to use the data of people without their consent or misuse it. To ensure the proper implementation of privacy **information security** is essential. Guidelines like the **ISO/IEC 27001** can be used, so that no regulations are being neglected. **ISO/IEC 27701** is an extension to ISO/IEC 27001 and aims to establish, implement, maintain, and continually improve a Privacy Information Management System.

The standard ISO/IEC 27001 also follows **laws** like the GDPR, so that implementing the ISO standard implies following the GDPR. These rules, laws, policies and regulations are all written down in the **regulatory compliance** of a company and have to be followed in order to avoid fines or other penalties. The regulatory compliance does not only include laws like the GDPR or COPPA, which protect the privacy and data security of people. Another part of regulatory compliance is the **data retention**, which means that data has to be archived and deleted after a certain time period. This is part of the **records management**, which is an ongoing cycle on how to handle data within a company. Auditing records management and assessing data retention regularly is done via **data auditing**. Furthermore it ensures regulatory compliance and following laws.

3 – Research

The following concept map aims to summarize the main ideas present in the GDPR:



Data Subject is an identifiable natural person is one who can be identified. **Data minimisation** states that the data used is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation** is the requirement that the collection and processing of personal data has a clearly defined purpose. **Storage limitation** is a principle that states that data collected and processed should not be held or further used unless this is essential. **Data controller** is the agent that determines the purposes and means of the processing of personal data. **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. **Supervisory authority** means an independent public authority which is established by a Member State. **Data accuracy** expresses the idea that the data used expresses the reality of the values faithfully. The **consent** of the data subject means any freely given, specific, informed and unambiguous indication of wishes by which the data subject, either by a statement or by a clear affirmative action, proclaims agreement to the processing of their personal data.

4 – Topic for discussion

What are the main mechanisms to maintain consistency of GDPR, in the context of national law, in different countries in Europe?