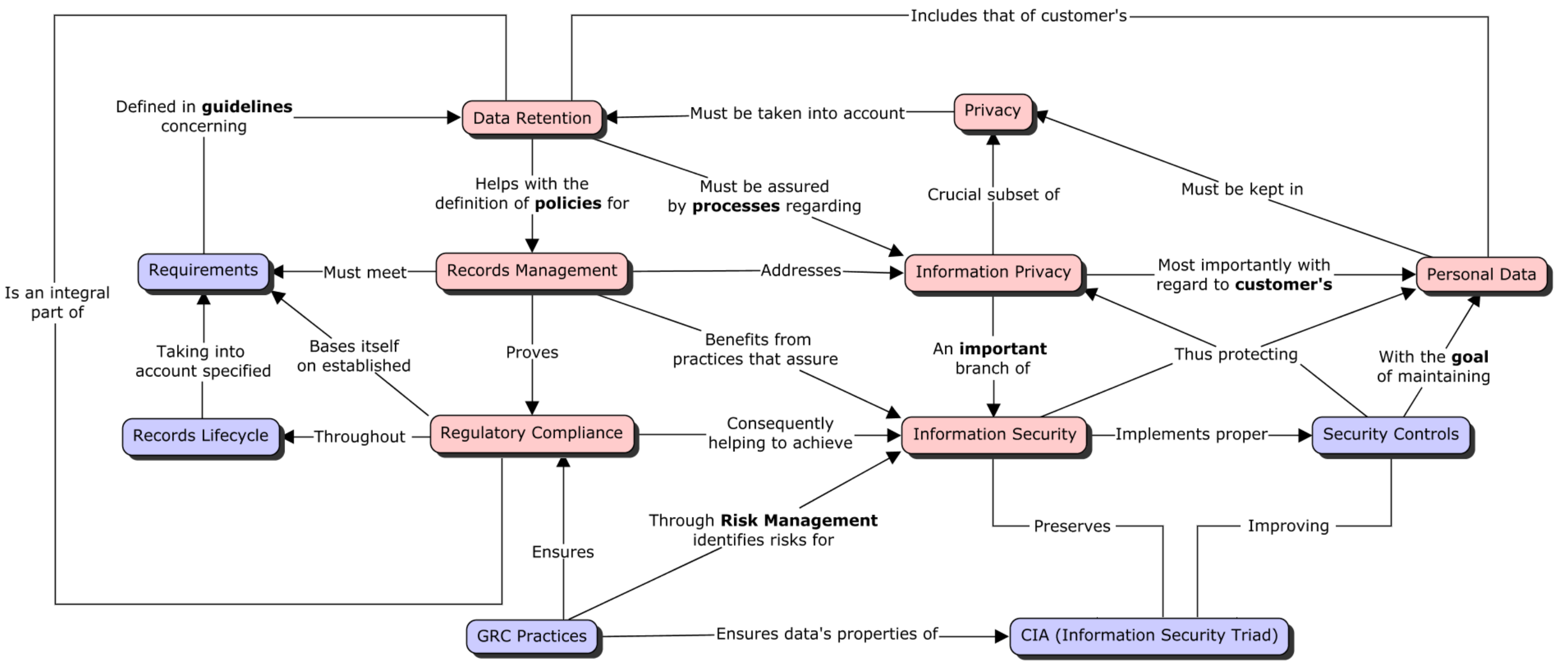
GSI (Case G) - Students numbers (5 digits): 82069 - 83779

1 – Conceptual analysis


Includes that of customer's
Defined in guidelines concerning
Data Retention
Must be taken into account
Privacy
Helps with the definition of policies for
Must be assured by processes regarding
Crucial subset of
Must be kept in
Is an integral part of
Requirements
Must meet
Records Management
Addresses
Information Privacy
Most importantly with regard to customer's
Personal Data
Taking into account specified
Bases itself on established
Proves
Benefits from practices that assure
An important branch of
Thus protecting
With the goal of maintaining
Records Lifecycle
Throughout
Regulatory Compliance
Consequently helping to achieve
Information Security
Implements proper
Security Controls
Through Risk Management identifies risks for
Preserves
Improving
Ensures
GRC Practices
Ensures data's properties of
CIA (Information Security Triad)

Concept	Definition (one sentence by concept)
CIA (Information Security Triad)	**Triad** that constitutes one of main pillars of knowledge about **Information Security**. The **three letters** stand for **confidentiality**, **integrity**, and **availability**. **Management**-wise this is used as a **model** to **evaluate** the **information security** of an **organization**.
Data Retention	The policies and guidelines of **persistent data** and **records management** for meeting legal and **business** data archival **requirements**.
GRC	The term that covers an **organization's** approach across the practices of **governance**, **risk management** and **compliance** enabling **organizations** to reliably achieve **objectives**, address **uncertainty** and act with **integrity**.
Information Privacy	**Relationship** between the **collection** and **dissemination** of **data** through **IT systems** usage and the **public expectation** of **privacy**, **legal** and **political issues** surrounding and including the sharing of information with third parties.
Information Security	Practice of preventing **unauthorized access**, **use**, **disclosure**, **disruption**, **modification**, **inspection**, **recording** or **destruction** of **information**.
Personal Data	Any type of **information** that relates to an **identified** or **identifiable** living **individual**.
Privacy	The state in which one is not **observed** or **disturbed** by other **people**, **secluding information** about themselves, thus **expressing** themselves **selectively**.
Records Lifecycle	Stages regarding the **lifespan** of **records**, which includes the **creation**, **preservation** in **archives** and **disposal**, in **organizations**.
Records Management	**Organizational** function dedicated to the **management** of **information** since its **creation** to its **disposition**, going throughout its whole **life-cycle**.
Regulatory Compliance	**Goal** that **organizations** aspire to **achieve** by ensuring they are **aware** of and **behave** in a proper way thus **complying** with **relevant laws**, **policies**, and **regulations**.
Requirements	A necessary **condition** or **capability** that must be met by the **service**, **product**, or **solution** to satisfy a **contract**, specification, or other formally imposed **documents**.
Security Controls	**Procedures** assuring that the **Information Security** practices that an **organization** is using operate as intended.

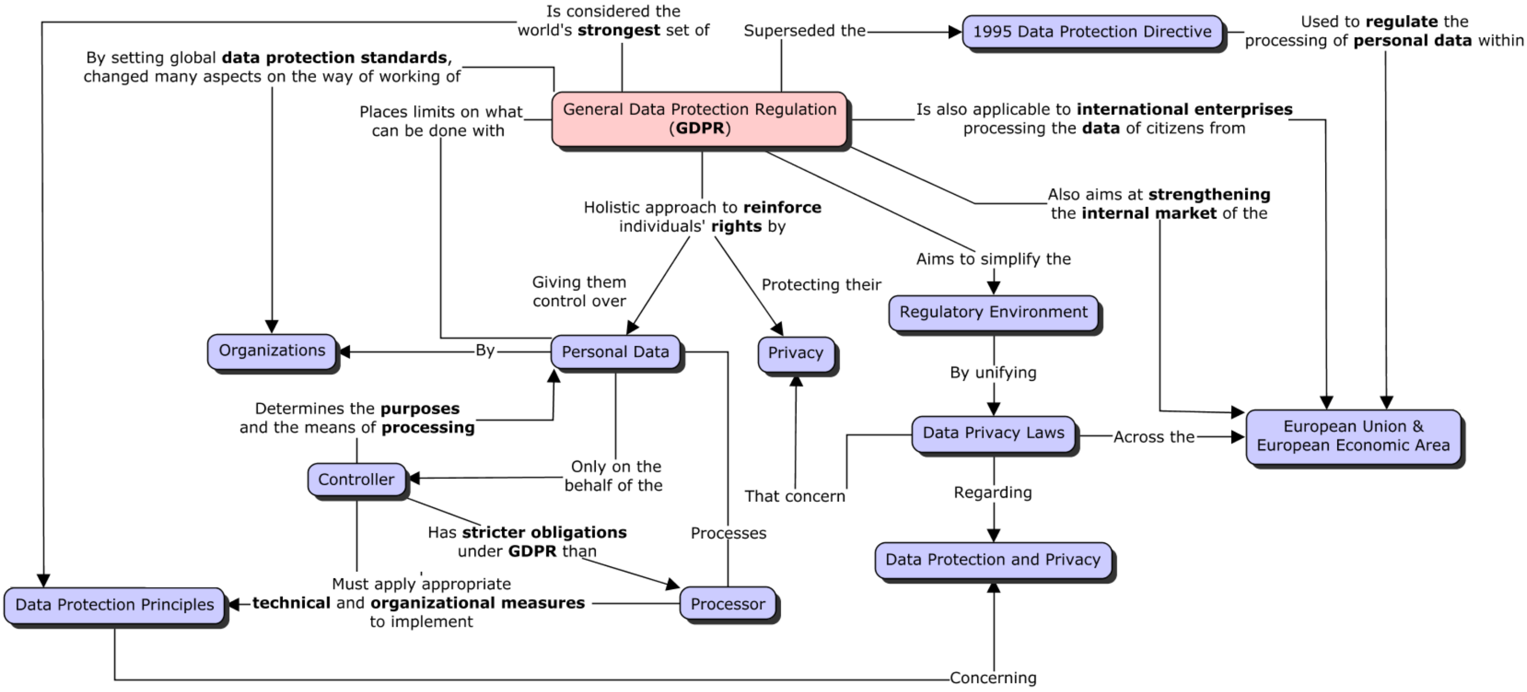
2 – Description of the analysis

With this concept map we plan on expanding upon the following points:

- The utmost importance for **organizations** to employ proper **Information Security** models and implement **effective controls** to guarantee the **privacy** of **information retained** in **IT Systems**. The application of these **security practices** follows the advent of large-scale and ever innovative **cyberattacks**, that have greatly **impacted** large scale modern **organizations**, through the **exposition** of **irresponsible data**-**handling** procedures that dealt major blows to their **integrity** and **public perception**.
- Moreover, **GRC practices** are applied with the **goal** of **preserving** the **confidentiality**, **integrity** and **availability** of stored data which, not only includes **organizational information**, but **customers**' **personal data** which must be **kept** in **privacy** and abide with an ever-growing number of nationwide **data protection policies** and **regulations**.
- Furthermore, we plan on expanding how **Records Management** addresses responsible **data retention policies** to guarantee the **privacy** of **information**, mainly **resources** and **records** kept by the **organization**. Nonetheless, these **management procedures** must comply with **regulations** and **ISO standards** to ensure proper **security** of **data** and **records retained** by an organization.
- How **management procedures** and **GRC practices** must meet **specific requirements** regarding the **handling** of **resources** throughout their **lifecycle** to assure **compliance** with established regulations and the preservation of the **confidentiality** and **integrity** of **data**.

Concluding, one can observe that the concept interlinking the remainder is that of **Information Privacy**. **Organizations** thus intend on **complying** with **regulations** regarding **records management** and **data retention policies**, to ensure efficient **information privacy** guarantees of **customers' personal data**, through the implementation of proper **security controls** that maintain **information's security** through the **assurance** of data's **confidentiality**, **integrity** and **availability** properties.

3 – Research


Is considered the world's **strongest** set of
Superseded the
1995 Data Protection Directive
Used to **regulate** the processing of **personal data** within
By setting global **data protection standards**, changed many aspects on the way of working of
Places limits on what can be done with
General Data Protection Regulation (**GDPR**)
Is also applicable to **international enterprises** processing the **data** of citizens from
Also aims at **strengthening** the **internal market** of the
Holistic approach to **reinforce** individuals' **rights** by
Aims to simplify the
Giving them control over
Protecting their
Regulatory Environment
Organizations
By
Personal Data
Privacy
By unifying
Determines the **purposes** and the means of **processing**
Data Privacy Laws
Across the
European Union & European Economic Area
Controller
Only on the behalf of the
That concern
Regarding
Has **stricter obligations** under **GDPR** than
Processes
Data Protection and Privacy
Data Protection Principles
Must apply appropriate **technical** and **organizational measures** to implement
Processor
Concerning

4 – Topic for discussion

Given the ongoing **coronavirus** pandemic, discussing **Data Retention**, **Records Management** and **Personal Data** is more important than ever. Where does the **ethical line** stand, between the usage of **Personal Data** regarding **infected patients** that could be used to define **models** that could help **mitigate the spreading,** and the **retention** of these **records** for a **large period** of **time**? How are these practices affected by the **GDPR**? These regulations are being deeply discussed nowadays, particularly in countries that are trying to get back to normality and started to use **tracking-related applications** to surveil their citizens. Hence the pertinency of our question.