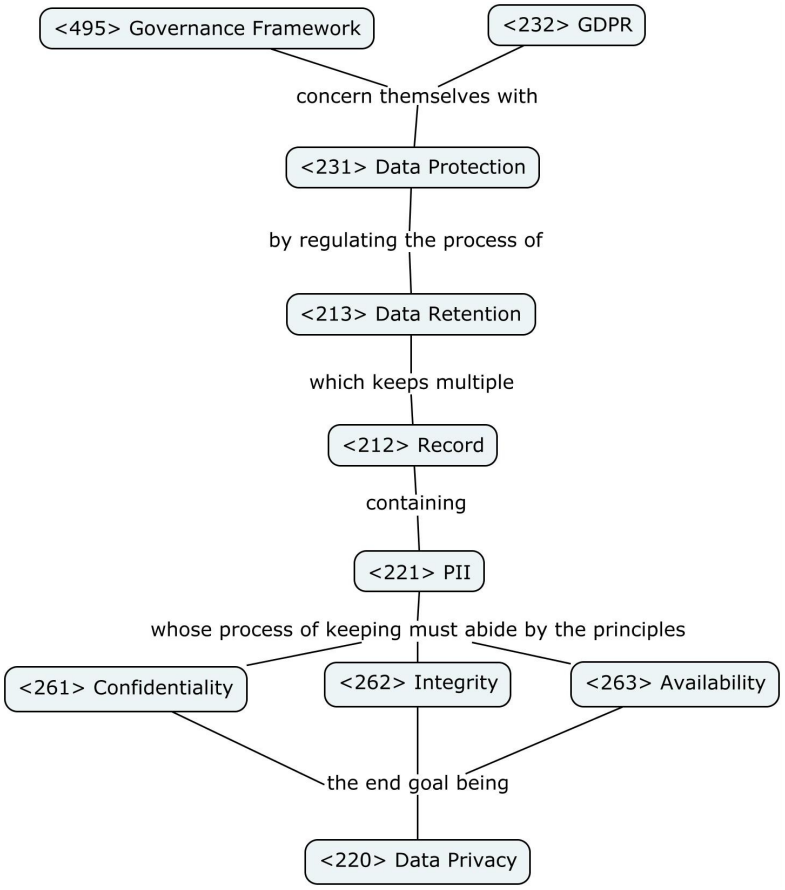
Maria Campos 95629

GDPR & DGA

CMAP and Description



Concept	Definition
<495> Governance Framework	A governance framework is a set of rules and guidelines that help an organization run smoothly by telling people what they should do, how decisions are made, and who is responsible for what. Ensures everyone knows what they're supposed to do and keeps things organized. It helps the organization work well and achieve its goals. [5]

DGA, as a **Governance Framework**, and the **GDPR** law concern themselves with safeguarding information from compromise, achieving **Data Protection**. To do this, they regulate how **Data Retention** is performed and how a **Record** that contains **Personally Identifiable Information (PII)** is transferred by stating how the process of keeping these records must abide by the principles of **Integrity**, **Confidentiality** and **Availability.** This makes it so that data is protected against unauthorized access, loss, or damage, granting the citizens the right to control and know how their information is used - **Data Privacy.**

Maria Campos 95629

Description of the Subject

GDPR (General Data Protection Regulation) is a regulation in EU law on **data protection** and **privacy** constituting a component of the Human Rights Law. The main concern is regulating the transfer of personal data in order to grant the individual control over their own personal data. [1]

Article 6 states that personal data may not be processed unless there is at least one legal basis to do, there are six lawful purposes:

- (a) If individual has given consent to the processing of their personal data;
- (b) To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- (c) To comply with a data controller's legal obligations;
- (d) To protect the vital interests of a data subject or another individual;
- (e) To perform a task in the public interest or in official authority;
- (f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

GDPR has 7 key principles[2]:

1 - **Lawfulness, fairness and transparency** - **personal data** must be processed based on a legal basis, taking into account the rights and interests of individuals, and clear and transparent communication about the data processing activities;

2 - **Purpose limitation** - personal data should only be collected for specific and legitimate purposes, and it should not be further processed in a manner incompatible with those purposes;

3 - **Data minimisation** - processing of only necessary and relevant personal data, avoiding unnecessary data collection;

4 - **Accuracy** - personal data is kept up to date, corrected when necessary, and reasonable measures are taken to ensure the information is accurate and complete;

5 - **Storage limitation** - personal data should be retained only for as long as necessary for the purposes for which it was collected, and securely deleted or anonymized when it is no longer needed;

6 - **Integrity and confidentiality (security)** - personal data is processed in a secure manner, protecting it against unauthorized access, loss, or damage, and maintaining its accuracy and reliability;

7 - **Accountability** - the responsibility is on data controllers to demonstrate **compliance** with **GDPR principles**, implement measures to ensure **data protectio**n, and maintain **records** of their data processing activities.

DGA (Data Governance Act) is a legislative proposal of the European Commission that has the goal of creating a framework to facilitate data sharing. It deals with all kinds of that be it data of public bodies, private corporations or citizens. [3]

The key **goals** of DGA[4] are:

- **Data Altruism:** promotes voluntary data sharing for societal benefit, such as research and public health.
- **Data intermediaries:** trusted entities enable secure data sharing between parties while ensuring **compliance** with **data protection rules**.
- **Data sharing mechanisms:** aim to establish standardized and secure technical measures, such as APIs, to facilitate the exchange of data while maintaining data protection and privacy.
- **Strengthening data portability:** aims to bolster individuals' control over their data by facilitating seamless transferability between service providers, promoting data mobility and user empowerment.
- **Enforcement and sanctions:** proposes enforcement mechanisms and administrative fines to ensure compliance with data governance obligations, establishing consequences for non-compliance.

In conclusion, both GDPR and DGA prioritize safeguarding personal data and promoting responsible data governance. The difference is that GDPR focuses on protecting citizens’ privacy rights and the DGA seeks to create a framework for secured data sharing. When seen together, these two regulations establish a foundation for data protection and governance, allowing accountability in the digital economy and enabling innovation and economic growth in the EU.

References

[1] General Data Protection Regulation [Online]
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[2] What is GDPR? The summary guide to GDPR compliance in the UK [Online]
https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
[3] Data Governance Act [Online]
https://en.wikipedia.org/wiki/Data_Governance_Act
[4] Data Governance Act explained [Online]
https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
[5] Governance framework [Online]
https://en.wikipedia.org/wiki/Governance_framework