# Data governance Dictionary:

3 overall roles (there can be more if you want)

Data Owner (Senior lvl, only one data owner from each department)

* Business leaders with overall responsibility for data. They set policies and guidelines for their datasets
* Don’t have the time to always act in response to the data.
* Often delegates the work to the data steward.
* Bear responsibility for data privacy. (Could come from legal, ethical or contractual obligations), could require the formal designation of a DPO (Data protection officer) to be valid.

DPO (Data protection officer) (Ikke altid skal ens virksomhed have en DPO)

* Skal sørge for at GDPR er overholdt.
* Behøves ikke at være der, hvis der ikke bliver behandlet personlige oplysninger i et stort omfang eller der ikke bliver behandlet personfølsomme personoplysninger.
* Skal sørge at DPO kan udføre sit arbejde uden forstyrrelse n for generelt managment.

Data Steward (there can be multiple data stewards)

* Handles the day-to-day governance activities.

Data Custodian (Often IT personnel, cuz they are system administrators often)

* Actually, store and process information
* Makes sure that proper data protection services are in place (Encryption, Backups, Access controls and other mechanisms that meets the requirements set forth by the data stewards / data owners)

Steward roles:

Data Controllers

* Determine the reasons for processing personal information and direct the methods of processing

Data Processors

* Service providers that process personal information on behalf of a data controller
* Bear responsibility for data privacy.

Data at rest

* Data stored on a local drive, on a shared file server, or in a cloud service.

Data in motion

* Data transmitted over a wired or wireless network.

Steganography

* Hides data inside of images or other files.

AAA

* (Identification)
* Authentication
* Authorization
* Accounting

The data lifecycle

* Create
  + The organization created new data / modificated data.
* Store
  + The organization store the data.
* Use
  + The active use of data
* Share
  + Data is made available to others.
* Archive
  + Retained in long term storage.
* Destroy
  + Data is destroyed. Should be destroyed using a secure destroying technique.

Data Sanitization

Privacy Policy

* External
* Explains to employees what their responsibilities are, when handling personally identifiable information

Acceptable use policy.

* Internal
* That describes the organization’s privacy practices to data subjects.

Privacy program mechanisms.

* Procedures for distributing privacy notices.
* Mechanisms for tracking user preferences.
* Logging and auditing capabilities for accountability

Data inventory

PII (Personal Identifiable Information)

* Any information that can be used to distinguish an individual’s identity or any information that is either linked or linkable to an individual.