Data Protection

Intellectual Property -> Creation of the mind like inventions, designs, symbols, literary works, artistic works, protection involves right management, strict access controls, and potentially watermark.
Copyright protects:

- Literary works
- Musical works
- Dramatic works
- Pantomimes and choreographic works
- Pictorial, graphical, and sculptural works
- Motion pictures and audiovisual works
- Sound recordings
- Architectural works

Regulated Data -> Data that is subject to regulatory requirements, such as personal data protected under laws like GDPR, health information covered by HIPAA, or financial data under PCI-DSS. Compliance with legal and regulatory standards is crucial.
Legal Data -> Information pertaining to legal matters, including case files, legal advice, and other sensitive legal documents
Financial Data -> Financial records, credit information and other monetary data

Human-Readable Data -> Easily interpretable by humans
Non-Human Readable Data -> Require specific software to help read (0 and 1 language)

Data Classification -> Help in determining the level of security controls and handling protocols that should be applied. The owner of the data must assign to information
Classification level by military and government:

- Unclassified -> No protection needed
- Confidential -> Filing cabinet with a metal bar and lock
- Secret -> An approved safe
- Top Secret -> A vault

Other example:

- Public -> Public information on the website
- Sensitive -> Profit earning and forecasts, financial information
- Private/Restricted -> Work history, human resource information

- Confidential/Proprietary -> Trade Secret, Health care information, technical specification of a product
- Critical -> If compromised, could lead to severe harm or damage to an organization

Data Sovereignty -> Follow the law of the people/system you collect data, if you collect data from people from US and store in Brazil you will need to follow US privacy data laws

Methods to secure data:

- Encryption
- Hashing
- Masking -> Process that protect sensitive data by replacing, hiding, or scrambling data with fictional or anonymized data (123-xxx-7890) data is modified forever, this makes more appropriated for DEV env IT IS NOT CONSIDER ENCRYPTION
- Salting -> Add random values to a password before hash to prevent the same input from generating the same hash value
- Tokenization -> Replace sensitive data with non-sensitive substitutes (randomly generated), knows as token data is NOT modified forever, this makes more appropriated for PROD env
- Obfuscation -> Make data ambiguous or unclear to obscure, it involves techniques such as renaming variables, adding unnecessary code, and restructuring the code
- Steganography -> Concealing a message, image or file within another message, image or file (secret messages in files) add message in the metadata of a image
- Segmentation
- Permission restriction

Data controller -> Organizations that determine the purposes and means of processing personal data - YOU
Data processor -> Process personal data on behalf of data controllers - GOOGLE
Data subjects -> Individuals whose personal data is being processed by organizations - USERS
Data custodians/stewards -> Responsible for the day-to-day management and protection of data assets, as directed by the owner
Visitor (Data subject) visit your website (Data controller) because of Google Analytics (Data processor) ad.