Information Systems

Chapter-6

Data Privacy Fundamentals

-Sanket Mohan Pandhare

Data Privacy Definition

- Data privacy is the branch of data management dealing with sharing data with third parties. It is generally based on protecting consumer information and giving consumers the right to keep their information from other organizations without consent or knowledge of this fact.
- Data privacy is about setting different levels of controls to protect this information from third parties, getting consent from data subjects when necessary, and maintaining data integrity.
- The fundamentals of data privacy include data confidentiality, data security, limitations in what data is collected and used, transparency in how the data is used, and compliance with the appropriate data privacy laws.

Cont.

- Data privacy fundamentals entail the proper use and handling of data with sensitive information. This typically includes personal, health, or financial data about an individual or organization. **It should not be confused with data security, which is the process of protecting data from being viewed, altered, or stolen by unauthorized users.**

Data Confidentiality

- Data confidentiality is the prevention of unauthorized entities from accessing sensitive data. Users who access the data must be properly authorized to use it, see it, and distribute it. Not all data is created equal in this regard, as some types of data are more sensitive than others.
- In the case of the General Data Protection Regulation (GDPR) in the European Union, data that is to be kept confidential, or that has stronger legal protections, includes race, ethnic background, political opinions, religious beliefs, genetics, biometrics, health information, and sex life or orientation.

Cont.

- In the United States, protected data includes health information, attorney-client information, credit card and other financial information, human subject research information, personally identifiable information such as Social Security numbers, and student grades and records. As well, the Children's Online Privacy Protection Act (COPPA) restricts the collection of personal information from children under 12.

- Data Privacy laws in Tanzania
  - https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

Data Security

- Data security ties into data confidentiality, as it ties into keeping unauthorized users from accessing data. When securing sensitive information, or data in general, organizations should abide by the CIA triad: confidentiality, integrity, and availability.

- Data confidentiality, as mentioned above, means that data is kept private. This is done through encryption, sending sensitive data over secure connections such as a VPN, having a solid security policy in place, and ensuring physical security, such as keeping data centers on-premises and shredding documents with sensitive information.

Cont.

- Data integrity means making sure that data has not been altered or tampered with. This is done through user management through the principle of least privilege. This means users can only access the minimum amount of data they need for their jobs.

- Data availability means having the data available for authorized users as needed. Denial of service (DoS) attacks can disable a data center, which means that an organization should keep backups.

Limiting Data Collection

- When following data privacy fundamentals, organizations should collect as little information as possible about their users. According to GDPR Article 5(1)(b), this means that sensitive data should only be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”

- Organizations should only collect data that they intend to use purposefully. A doctor’s office will need a patient’s weight, height, and age in order to provide a thorough service. An online retailer fulfilling an order for clothes, however, requires none of that information. Organizations that collect unneeded data put themselves at risk.

Data Privacy Transparency

- When collecting information about users, organizations should be transparent in how they plan to use their data, and what data they are collecting. This includes having:
- **Consent,** where users must opt-in before their data is collected and shared.
- **A privacy policy,** which outlines what data is collected, the reasons for data collection and use, the length of time the data is kept, other parties involved, and where the data will go. This policy should be prominently displayed and easily accessible by users.
- **Disclosure,** where users will be informed about the privacy policy, as well as other functions that store and share data.

Compliance

- There are several laws and regulations concerning data privacy, especially with the rise in prominent breaches of personal data.
- These include regulations like the EU's GDPR and the United States' Health Insurance Portability and Accountability Act (HIPAA). In the United States, individual states can have stricter privacy laws than the federal level, such as the California Consumer Privacy Act (CCPA).
- When collecting data, an organization must ensure that they are abiding by these laws. These regulations apply to users within their jurisdiction, which means that even United States organizations with employees or users in the EU must comply with the GDPR.

Data Privacy Vs Data Security

- In short, data privacy and data security are, by no means, the same terms. Data privacy is about proper usage, collection, retention, deletion, and storage of data. Data security is policies, methods, and means to secure personal data.
- So, if you are using Google Gmail account, your password would be a method of data security, while the way Google uses your data to administer your account, would be data privacy.

Cont.

- Think for **example of a window on a building**; without it being in place an intruder can sneak in and violate both the privacy and security of the occupants.
- Once the window is mounted it will perform a pretty decent job in **keeping unwanted parties from getting into the building**. It will, however, **not prevent them from peeking in**, interfering thus with the occupants' privacy. At least not without a curtain.
- In this (oversimplified) example the **window is a security control**, while the **curtain is privacy control**.
- The former can exist without the latter, but not vice versa. **Data security is a prerequisite to data privacy.** And information security is the main prerequisite to data privacy.

Data Privacy Vs Data Protection

- Data Privacy & Data Protection is like two faces of the same coin, where one is the legal aspect establishing rules & regulations, while the other is the technical aspect to ensure that these regulations are enforced correctly.
- Simply put, Data Privacy ensures that your rightful digital data is not sold to anyone, in a way to secure your right to Privacy, while Data Protection ensures that your data is not hacked or stolen.

Cont.

- Assume you have a wedding at home, and hence your house is bustling with lots of relatives. Amidst all the rush & hustle, you feel a need for some solitude & decide to go and sit in a room alone. To avoid people from barging in, you put a sign saying ‘Do not Enter’ on the Doorknob. But to ensure your privacy, (just in case someone doesn't see the sign, or decides to ignore it) you lock the door on the inside. Now, you feel completely safe in the room, ensured that your solitude cannot be disturbed.
- Now, there are two things here to consider, first ‘the sign at the door’, that acts as a way of letting people know that their presence is not required and the other one is ‘the lock’, which ensures that no one can enter, even if they try. One works to authorize your privacy, another works to ensure it.

Cont.

- Data Privacy establishes the authorization of your data, deciding who can or cannot access your data, how should your data be used & other things like the Sign on the doorknob, keeping people out.
- On the other hand, Data Protection means protecting your data from being used, hacked or stolen by unauthorized users, ensuring that even if someone tries to defy the regulations of Data Privacy, they can't misuse your data, much like the lock.
- Now, both these elements are interrelated in a way that **'Data Privacy can work only when Data Protection is taken care of, while the vice versa is not true.'**
- You can simply lock the door, without putting the sign to avoid people from coming in. But, you can't simply put a sign & expect everyone to abide by it.
- So, Data Privacy rules are only useful, when the companies are protecting your digital data, which they should.

GDPR Overview

- GDPR - General Data Protection Regulations
- Replaces Data Protection Act 1998
- Effective from 25th May 2018
- 11 chapters and 99 articles
- It’s a ‘Regulation’ – so we have the Articles (the law itself) and Recitals (explanatory note within the body of GDPR)

Definitions

- **Data Controllers & Data Processors**
- The data controller will be the one to dictate how and why data is going to be used by the organization.
- Controller says how and why personal data is processed.
- A data controller can process collected data using its own processes. Sometimes need work with a third-party or an external service in order to work with the data that has been gathered.
- A data processor simply **processes any data** that the data controller gives them.
- The third-party data processor does not own the data that they process nor do they control it.

Definitions

- **Processing**
- Basically assume any activity with personal data will be processing including:
  - Collecting
  - Storing
  - Using
  - Deleting
  - Sharing

Principles

- Data shall be:
- Processed lawfully, fairly and transparently

- Lawful – mustn't be in breach of other laws (e.g. common law duty of confidentiality) & must be lawful in accordance with Article 6 & 9 – Lawfulness of processing

- Fair & transparent – data subjects made aware (privacy notices etc.); must 'feel' fair.

Principles

- Data shall be:

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

Principles

- Data shall be:

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

Principles

- Data shall be:

- Accurate and, where necessary, kept up to date(accuracy)

Principles

- Data shall be:

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)

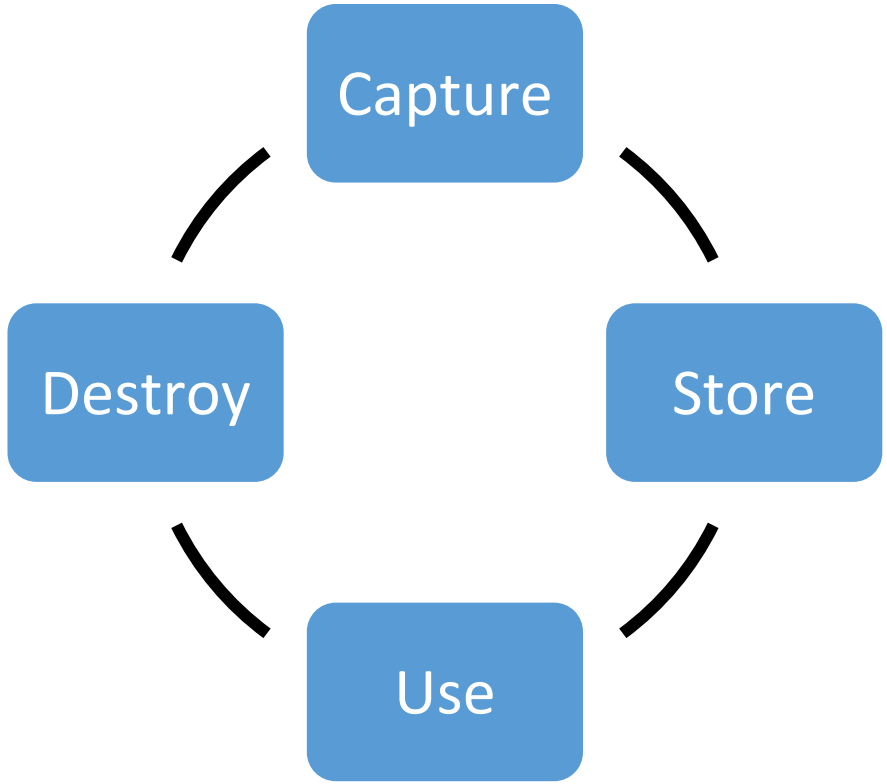
Principles

- Data shall be:

- Processed with appropriate security, including protection against
  - Unauthorised or unlawful processing
  - Accidental loss, destruction or damage
  - (Integrity and confidentiality)

Information Life Cycle

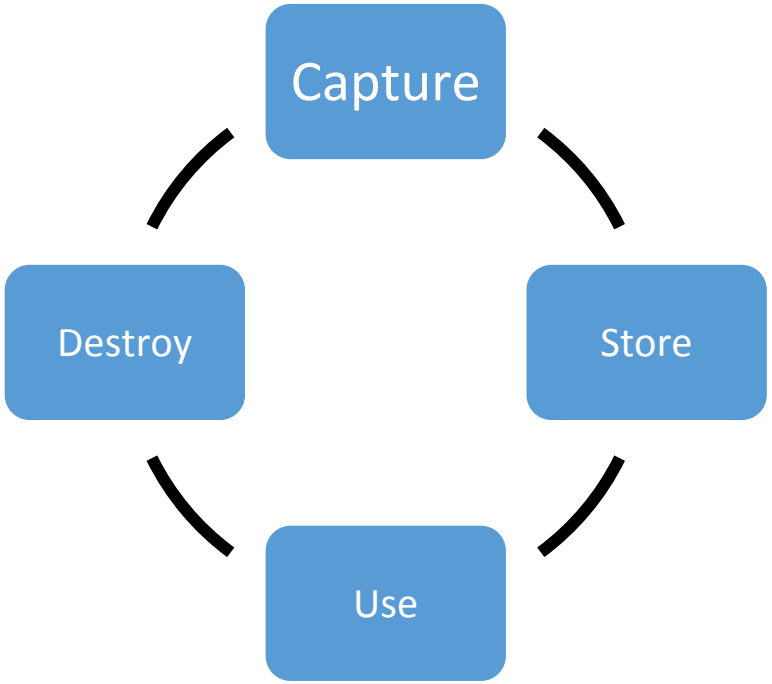
The diagram below illustrates four main stages in the life cycle of information



1. **Capture** – Obtain and record information
2. **Store** – Save the information electronically or in paper format
3. **Use** – Use or reuse information
4. **Destroy** – Delete, erase or shred information

GDPR Information Life Cycle

Under GDPR, the information life cycle will remain broadly the same, however there are additional factors to be considered at each stage



Capture

1. What you are allowed to capture
2. How you may do so
3. What you must tell the person in advance
4. What you must get from them (their permission)

Store

1. How you must store it
2. Where it can be stored
3. Obligations of third parties
4. What happens if you lose it

Use

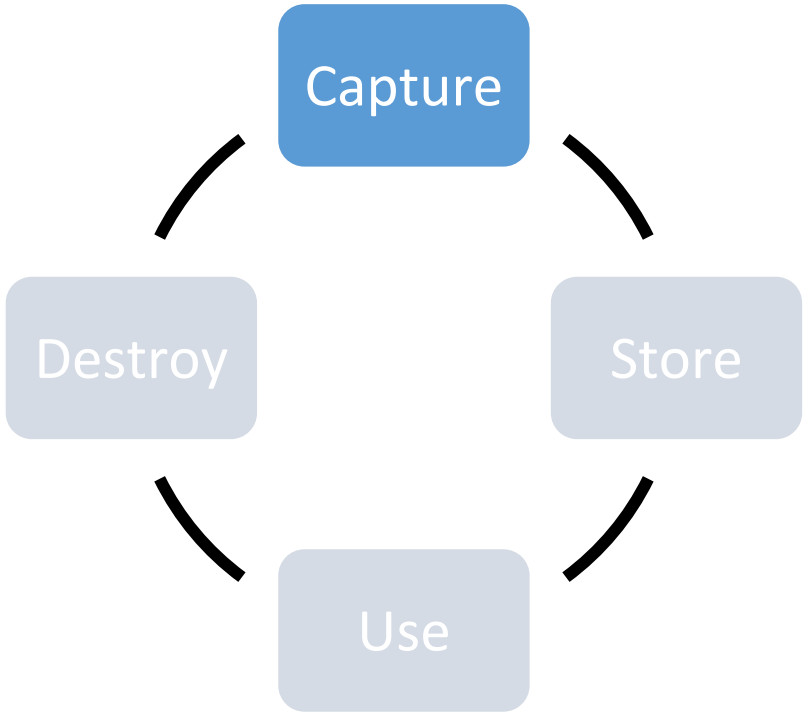
1. What you can use it for
2. What you can't use it for

Destroy

1. How long you can keep it for
2. When you must destroy information

GDPR Information Life Cycle

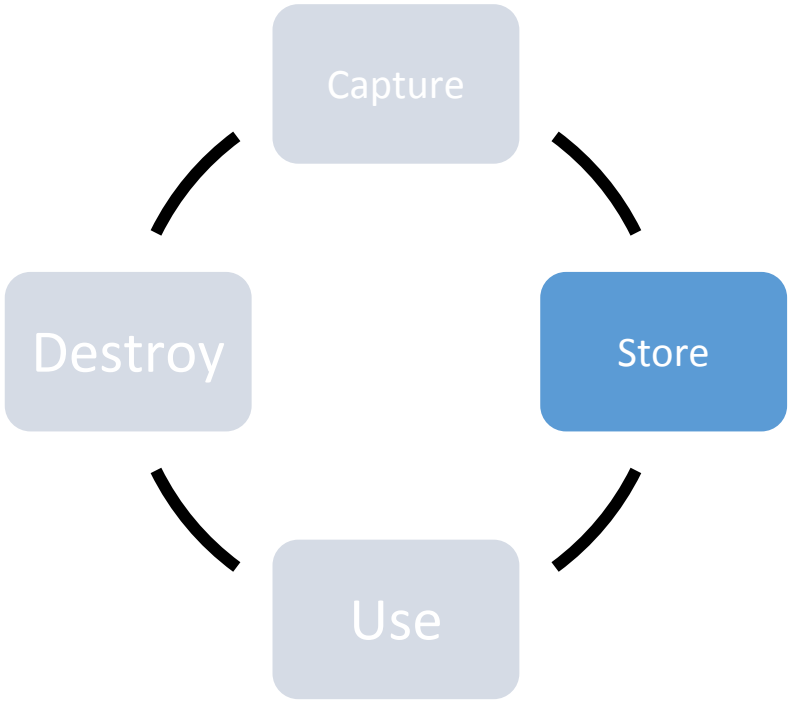
Capturing Information under GDPR



1. **Data Minimisation** (Only ask for what is needed)
2. **Privacy Notices** (Clearly inform what, why, who and where)
3. **Data Subject Rights** (state the persons rights under the legislation)
4. **Obtain Consent** (consent must be freely given and explicit for the purpose or purposes)

GDPR Information Life Cycle

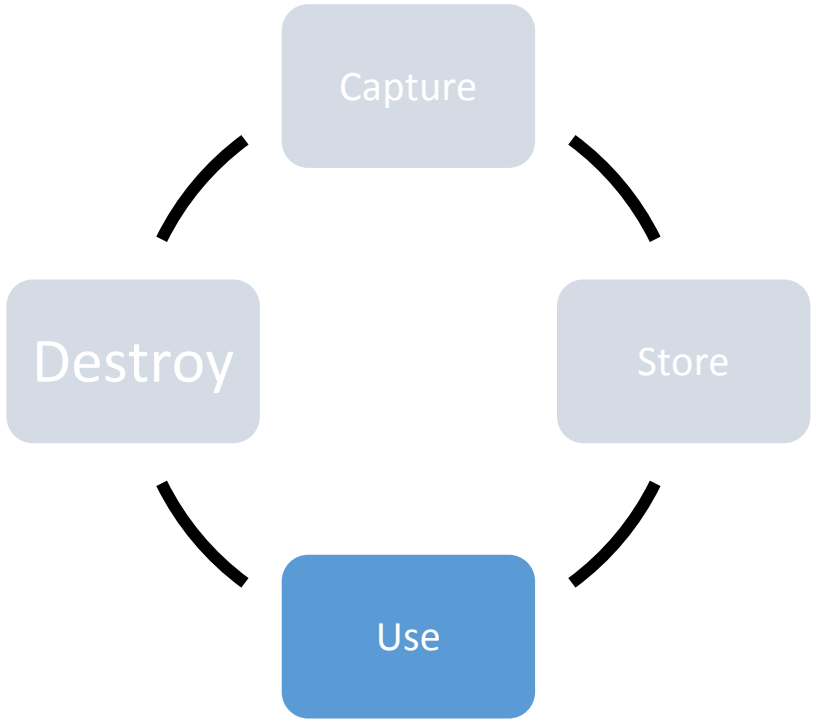
Storing Information under GDPR



1. **Safe and Secure** (Information must be stored appropriately e.g. locked cabinets/password protected files)
2. **Restricted Access** (Only authorised persons should have access to it)
3. **Data Inventory** (Information captured should be recorded)
4. **Subject Access Requests** (Must be in a position to provide ALL information held)
5. **Contracts with Data Processors** (Any third parties must have GDPR contracts in place)
6. **Data Breaches** (Processes to detect, report and investigate Data Breaches must be in place)

GDPR Information Life Cycle

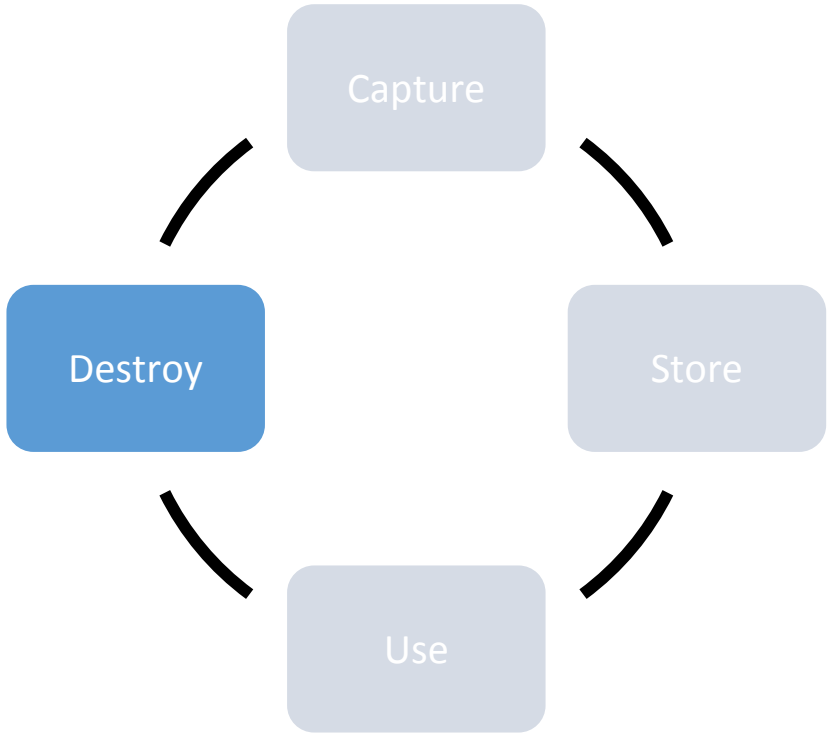
Use of Information under GDPR



1. **Appropriate use** (Must be for the purpose(s) originally stated)
2. **Consent** (Must have person's consent or a lawful basis for processing it)
3. **Manage Consent** (Individuals have the right to revoke consent for part or all of the processing, this must be managed)
4. **Restricted** (Profiling or automated decision making are restricted)
5. **International Transfers** (Any processing that occurs outside EU must have been communicated to person at time of data capture and must have additional safeguards in place)

GDPR Information Life Cycle

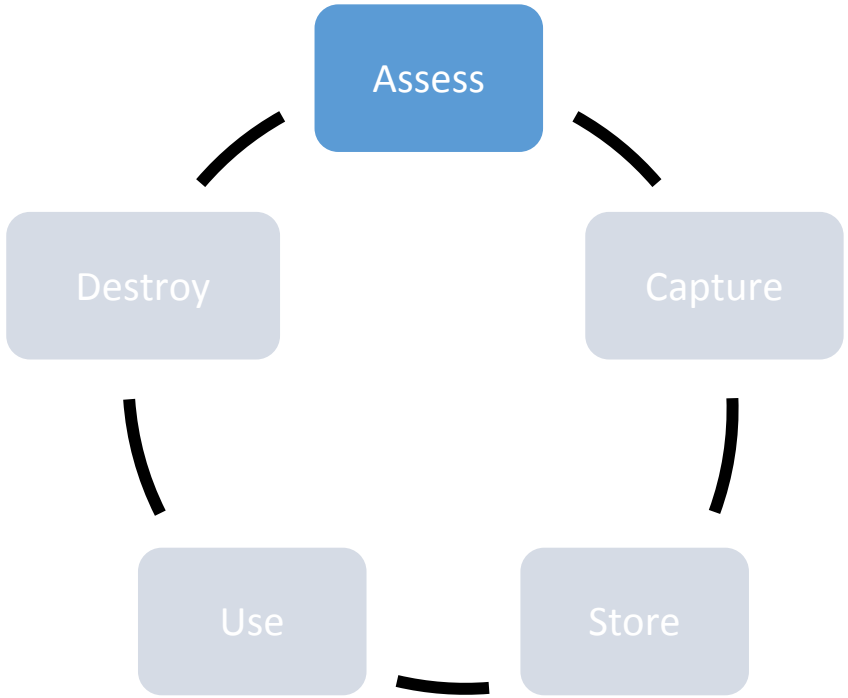
Destruction of Information under GDPR



1. **Retention Period** (Retention periods must be documented and justified and data must be destroyed after its useful retention period has expired).
2. **Right to erasure** (Must be erased upon request from person)
3. **Portability** (Must be provided in standard format)
4. **Third Party Copies** (All copies of information must be deleted including those held by third parties. Systems like Whatsapp can be an issue here due to the lack of control over the personal data held within it.)

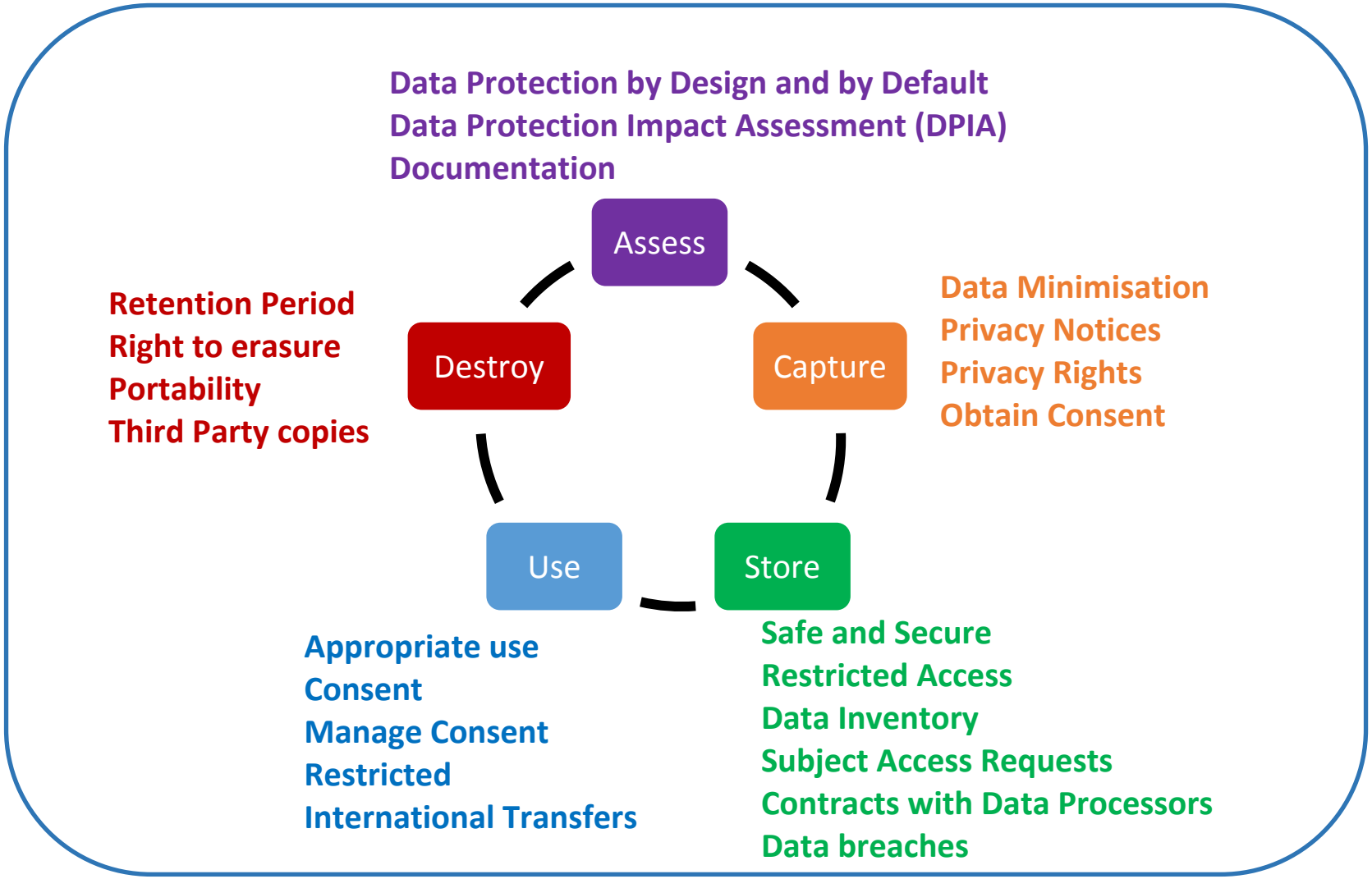
GDPR Information Life Cycle

There is a fifth step required under GDPR, that is the needed to ensure Privacy by Design through upfront assessment of relevant projects



1. **Data Protection by Design and by Default** (All relevant projects or initiatives must consider impacts on privacy from the outset)
2. **Data Protection Impact Assessment (DPIA)** (Must be conducted for new technology, profiling, large scale processing, or engagement of a new third party data processor)
3. **Documentation** (Decisions and rationale for decisions around Data Protection should be documented)

Summary of GDPR Information Life Cycle



Summary

- The fundamentals of data privacy include data confidentiality, data security, limitation in data collection and use, transparency in data usage, and compliance with the appropriate data privacy laws.
- Organizations should use security best practices when protecting sensitive data.
- Organizations should understand and comply with data privacy laws that protect their users.
- https://gdpr-info.eu/