

GDPR

10 Key Talking Points

10 PRINCIPLE COMPONENTS



1 TRANSPARENCY

Processors and controllers **must notify** data subjects **how and why** they collect and use their personal data. This must be stated in **plain language**, and in an **easily accessible format**.



2 CONSENT

- Consent must be informed, unambiguous, and freely given.
- An individual's consent can no longer be assumed by default without an affirmative action.
- Any consent documentation should be written in plain language and be as easy to revoke as it is to provide (the "opt-out" methodology).



3 NOTIFICATION AND ACCESS RIGHTS

The **GDPR** brings new notification and access rights concerning personal data. For example, organizations falling under the **GDPR** must notify data subjects about:

- Which personal data is processed.
- The source of the data and the purpose of processing.

They must also:

- Clearly explain that the data subject has the right to get a copy of personal data processed.
- Provide data electronically if the data subject requests it in electronic format for no fee. Data holders have 30 days to respond to the access request.



4 RIGHT TO BE FORGOTTEN

Processors and controllers under certain circumstances must now erase and stop distributing personal data if a data subject requests it, or:

- When data is no longer necessary for to the purposes for which it was collected.
- The data subject withdraws consent and there are no grounds for processing without consent.
- The data subject objects to the processing.
- If the data was processed unlawfully.

Some exceptions to this right apply e.g., if the controller has to retain the data due to a legal obligation or reasons of public interest.



5 RIGHT TO DATA PORTABILITY

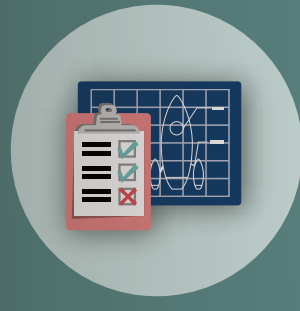
Processors and controllers must give data subjects their personal data in an electronic, structured, and commonly used format so that they can then provide the data to a third party if they choose. This is required where the processing is:

- Carried out on the basis of the consent of the person.
- Carried out by automated means.



6 BREACH NOTIFICATION

Processors and controllers must notify the appropriate Supervisory Authority of data breaches that are likely to put the rights of data subjects at risk within 72 hours of becoming aware of the breach.



7 PRIVACY BY DESIGN

Meeting "**privacy by design**" standards is a legal requirement of the **GDPR**, which essentially means that organizations must consider privacy guidelines and best practices at the very onset or design phase of a product or project that uses personal data rather than an afterthought.



8 UNIFORMITY

Because **GDPR** is a regulation, data protection rules are relatively uniform across EU with each country ensuring the rules are applied in a harmonized and effective way.



9 NON-EU COMPANIES

Non-EU companies that process personal data of **EU** citizens are subject to **EU** rules even if they are not located in Europe.



10 PENALTIES

The penalties for violating the **GDPR** can be severe: up to **20 million Euros** or **4%** of an organization's worldwide turnover.

DEFINING TERMS



Controllers

are government agencies and public and private organizations that collect and process personal data. They determine how and why it is collected, used and shared.



Processors

are companies or entities that process personal data on a controller's behalf, such as a third party IT contractor or cloud provider.



Data Subjects

are the individuals whose personal data is processed – they may be clients, employees, or customers – essentially any individual with whom our organization comes into contact with or collects information about.