ADGM

DATA PROTECTION BY DESIGN AND DEFAULT

What is Data Protection by Design?

An approach that ensures you consider data protection at the initial design phases of any system, service, product, or process, and then subsequently throughout the lifecycle.

Under the Data Protection Regulations, Data Controllers are required to:

- Integrate the necessary technical and organizational measures to ensure data protection principles are implemented effectively.
- Incorporate data protection into all processing and business activities, beginning with the design phase and continuing throughout the lifecycle.
- Keep data protection and privacy in mind in everything you do. This can assist you in adhering to fundamental requirements of the Regulations.

Data Protection by Design is applicable in a number of scenarios such as:

- When creating new IT systems, services, or products that process personal information.
- When designing privacy-related corporate policies, processes, or strategies.
- When collaborating with external parties involving data sharing.
- When using personal data for new purposes or internally using data in a different way.

What is Data Protection by Default?

Data protection by Default ensures that data is processed to achieve a specific purpose. It is tied to key data protection principles such as data minimization and purpose limitation. Data protection by Default requires that you to specify and implement data protection controls before the processing starts, appropriately inform individuals, and only process the data that is necessary for the purpose.

- Ensure you prioritize data protection when defining system and application default settings
- Provide individuals with sufficient controls and options to exercise their rights
- Ensure you provide clear information to individuals relating to the data that is being processed
- Process additional data only if the individual decides to approve or a valid legal basis can be relied upon
- Ensure that personal data is not processed unfairly which includes publishing information without consent

Who is responsible for implementing Data Protection by Design and Default?

The Data Protection Regulations specify that a Controller is responsible for implementing Data Protection by Design and by Default. Controllers are held accountable to implement the required measures and to do so in a demonstrable manner.

What is required when it comes to Data Processors?

The Data Protection Regulation specifies that Processors need to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Regulation and will ensure the protection of the rights of the Data Subjects. Controllers must ensure that careful considerations and due diligence is taken whenever appointing Processors. For example, you must only use Processors that provide sufficient guarantees to implement appropriate technical and organizational measures.

What are the underlying concepts of Data Protection by Design and by Default?

Proactive and preventive
Assess, identify, manage, and prevent any data protection risks before they materialize

End-to-end security
Incorporate best practice security features and practices from the point that personal data is collected until it is removed from the system

Data protection as the default
Be responsible for protecting individuals' personal data and provide data protection as a default setting

Transparency
Inform customers what personal data is collected from them and how it is being used

Data minimization
Only collect, store, and use personal data that is relevant and necessary

User-centric
Develop and implement data systems with individuals in mind and make the system user-friendly from a privacy perspective

Risk Minimization
Design and implement the right processes and relevant data security measures when processing personal data