TECH HIVE ADVISORY

MOROCCO'S CNDP RELEASES GUIDANCE ON DATA PROTECTION IMPACT ASSESSMENT

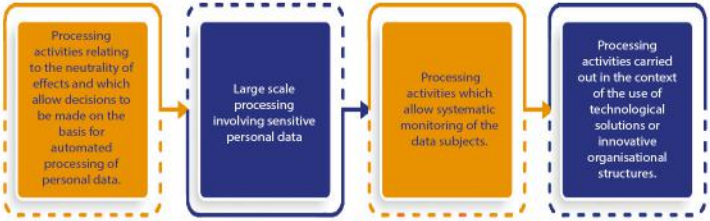
Morocco's Data Protection Authority, the National Commission for the Protection of Personal Data (CNPD) has released its deliberation on Data Protection Impact Assessment (DPIA). The deliberation is available here: https://tinyurl.com/y7oebzqk

A DPIA is a risk analysis technique, "which companies can systematically assess and identify the privacy and data protection impacts of any products they offer and the services they provide. It enables them to identify the impact and take the appropriate actions to prevent or, at the very least, minimise the risk of those impacts."

Key Provisions

- Processing must assess need and proportionality. Principle of proportionality must be respected at all stages of processing and understood before commencing the processing activity.
- Evaluate the risk of managing the rights and freedoms of individuals related to the processing of their personal data.
- Implement data minimisation.
- Impact assessment must be conducted before deploying a product or implementing a solution.
- Implement privacy by design and privacy by default.
- Evaluate security risk to processing personal data.
- The DPIA should be reviewed regularly in order to ensure that the level of risk remains acceptable.
- The data controller must comply with the accountability principle by demonstrating the evidence of compliance. A copy of the DPIA must be presented to the CNDP for validation before deploying the product or services. Besides, the controller must be able to present the DPIA in case of an audit being conducted by the CNDP.

Processing activities requiring DPIA



TECH HIVE ADVISORY

Content of a DPIA

A detailed description of the processing operations and their purposes, including both technical and operational aspects;

An assessment, of a more legal nature, of the necessity and proportionality of processing operations concerning fundamental principles and rights (purpose, data and retention periods, information and rights of individuals, etc.);

A more technical assessment of the risks to data security (confidentiality,integrity and availability), and their possible impacts on privacy, which makes it possible to determine the technical and organisational measures necessary to data protection;

A description of the measures envisaged dealing with the risks (measures of a legal, organisational, logical security and physical security), including the guarantees and mechanisms aimed at ensuring the protection of personal data personnel and demonstrate compliance with the law.

CNDP also recommends setting out the actors concerned when carrying out an impact analysis, and they are:

- the data controller who is the natural or legal person who determines the purpose and means of processing;
- the subcontractor (s) involved in the processing, who must provide their assistance and information necessary to carry out the impact analysis;
- the persons concerned by the processing, who can be consulted by the controller and formulate their opinions, in particular through a survey, poll, formal question to employee representatives; and
- depending on the context, the trades (project management), the teams responsible for implementation (project management), and the person in charge of systems security of information.