Deliberation n ° D-188-2020 dated 14/12/2020 governing the impact assessment relating to data protection (AIPD)

The CNDP (National Commission for the Protection of Personal Data Staff),

Under the chairmanship of Mr. Omar Seghrouchni;

Taking into consideration the observations of the members Ms. Souad El Kohen, Gentlemen Driss Belmahi, Abdelaziz Benzakour, Brahim Bouabid;

Considering article 24 of the Constitution of the Kingdom which provides that: "Everyone has the right to protection of his privacy ";

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automated processing of personal data to which the Kingdom of Morocco has joined on 05/28/2019;

Considering the law n ° 09-08 promulgated by the Dahir 1.09.15, of February 18, 2009, relating to the of natural persons with regard to the processing of personal data (BO n ° 5714 of 05/03/2009);

Considering the internal regulations of the CNDP (approved by decision of the Prime Minister n ° 3.33-11 of March 28, 2011 (BO n ° 5932 of 04/07/2011);

Having regard to the observations of Madame Souad El Kohen, Messrs Driss Belmahi, Abdelaziz Benzakour and Brahim Bouabid, rapporteurs appointed by the Commission.

The CNDP recalls that under the provisions of Articles 23 et seq. Of Law 09-08, this deliberation lays down the principles to be observed for the assessment of risks harmful to life privacy and the protection of personal data that may arise as a result of a treatment given.

Taking into account the international legal framework and good practices governing analyzes impact on data protection, the CNDP intends to promote the principle of empowerment of the entities concerned, in order to support them in their approach identification and assessment of situations likely to present the most risk for the rights and freedoms of the persons concerned.

To do this, the CNDP adopts the following principles and guidelines:

Definitions

- By data protection **impact assessment** , hereinafter referred to as impact analysis, the CNDP intends a process whose purpose is to describe a processing, to assess the necessity and proportionality thereof and to help

risk management for the rights and freedoms of individuals related to processing of their personal data, evaluating them and determining the measures necessary to deal with it.
It is an important tool with regard to the principle of responsibility, given the its usefulness for data controllers, not only for the purposes of implementation of data processing that respects privacy, but also for establish their ability to demonstrate that appropriate measures have been taken to ensure their compliance with law: namely the minimization of the data collected, the obligation to secure the latter, respect for Privacy by design and Privacy by default.

- A **risk** to privacy is a situation that describes a feared event (infringement the confidentiality, availability or integrity of data, and its potential impacts on the rights and freedoms of individuals) and its effects (all threats that would allow it to occur), estimated in terms of severity (for people involved) and probability.

Risk management can be defined as a set of activities coordinated in order to lead and manage an organization vis-à-vis the risk.

- The **proportionality** of the data processing, means its relevance with regard to of the legitimate aim pursued, and of its limitation to what is necessary with regard to the interests, rights and freedoms of the persons concerned or the public interest. He ... not must not lead to a disproportionate interference with those interests, rights and freedoms. The principle of proportionality must be respected at all stages of processing, including understood at the initial stage, i.e. when it is decided whether or not to proceed with the data processing.

Context of use

Data Protection Impact Assessment (DPIA) is used in different contexts by other regulations. It is used, in particular, to materialize the responsibilities in the context of regulations based on the principle of "Accountability" or empowerment. In this case, the Impact Assessment relating to Data Protection (AIPD) is established by the Data Controller who must present, in the event of an audit, to the authority in charge of the protection of personal data staff. In the case of sensitive processing, the list of which is specified by the

control, the Data Protection Impact Assessment (DPIA) is presented for validation, prior to any deployment of these treatments.

The regulations in Morocco are based on the declaration regime and could evolve towards that of "accountability" deemed to be more flexible and better aligned with the needs of the digital ecosystem. However, this development must be prepared, structured and based on clear principles and effective implementation and transparent, by the Data Controllers. The CNDP (National Control Commission of the protection of Personal Data) is part of this logic of simplification in order to promote support for Data Controllers in the deployment of this culture of accountability and a posteriori control.

The Data Protection Impact Assessment Study (DPIA) is an Analysis tool of Risks on Privacy. The principle of proportionality is applied according to the context operational and privacy requirements, approved by the Supervisory Authority, zero risk does not exist.

Thus, in anticipation of potential regulatory changes, the CNDP (Commission Nationale control of the protection of Personal Data) wishes to promote the principle of risk analyses in the field of privacy protection.

To do this, the Commission encourages:

- Subcontractors to formalize Impact Analyzes relating to the Protection of Data (AIPD) in order to simplify the files of compliance with Law 09-08 of their clients. These DPIAs would be referenced with the Commission, without being considered as constituting any authorization for implementation since the client final, remains at this stage fully responsible for the integration of the sub-system dealing in its ecosystem. This arrangement will optimize and promote standardization of the examination of notification files by facilitating the study of characteristics of the treatments managed by the subcontractors.
- Data controllers to set up Impact Analyzes relating to the Data Protection (AIPD), in the case of the processing defined below, with a view to better explain the measures taken to protect personal data personnel to the persons concerned and also in order to facilitate their exchanges with the CNDP (National Commission for the Protection of Personal Data Staff).

Treatments concerned

The CNDP establishes the lists of processing operations concerned and not concerned by this deliberation. These lists are evolving and will be regularly updated, according to its assessment of risks that certain transactions may present.

- *Treatments concerned*

  Mainly, the treatments presumed to involve a risk of harm to the protection of privacy and personal data, which are part of one or more of the following categories:

  - processing that contravenes compliance with the provisions of article 11 of law 09 - 08, relating to the neutrality of the effects and which allow decisions to be made on the basis for automated processing of personal data;

  - large-scale processing of sensitive data which, under Article 1 of law 09-08, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the person concerned or relating to his health, including his genetic data;

  - processing which allows systematic monitoring of the data subjects;

  - processing carried out within the framework of the use of technological solutions or innovative organizational structures.

  This list also extends to the treatments carried out:

  - in the context of compliance with a legal obligation to which the person responsible is subject processing;

  - within the framework of the performance of a mission of public interest or relating to the exercise of the public authority vested in the controller;

  - on the basis of a legal basis which regulates them.

Thus, an impact assessment is not necessary when the nature, scope, context and purposes of the intended processing are very similar to processing for which an impact assessment has already been carried out by the data controller or by a third party (authorities, public bodies, group of data controllers, etc.), and that its results can be reused and transposed.

Carrying out an impact analysis

An impact analysis must be carried out upstream, in a logic of anticipation before the implementation of the planned treatment. It must be reviewed on a regular basis, in order to ensure that the level of risk remains acceptable. It can relate to an operation or a set of similar processing operations and must contain at least:

- 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 with regard to fundamental principles and rights (purpose, data and retention periods, information and rights of individuals, etc.) no negotiable, fixed by law and to be respected whatever the risks;

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

- a description of the measures envisaged to deal with the risks (measures of a legal, organizational, 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.

Stakeholders concerned

The process of carrying out an impact analysis must involve all the actors of a processing concerned, namely and in a non-exhaustive manner:

- 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 for carrying out the impact assessment;

- the persons concerned by the processing, who can be consulted by the controller and formulate their opinions, in particular by means of a survey, poll, formal question to staff representatives;

- 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.

The CNDP recommends informing the contributions of all the actors solicited, as well as the choice failure to seek the opinion of a particular actor.

An impact assessment can usefully lead to the production of a report or a summary, that can be shared, published and communicated. This good practice contributes to the improvement trust and transparency between stakeholders.

Conclusion

A controller may use the performance of an impact assessment to support its notification file. The CNDP, in its support mission, and after instruction of the request submitted, recommend the measures to be considered by the data controller, that it deems sufficient to ensure a level of data protection of a adequate staff.

Rabat, December 14, 2020
Omar Seghrouchni
President of the CNDP