Deliberation 2018-326 of October 11, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday November 07, 2018 NOR: CNIL1829637X impact relating to data protection (AIPD) provided for by the general regulations on data protection (RGPD) The National Commission for Computing and Liberties,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, in particular its articles 35 and 36;

Having regard to the amended law of January 6, 1978, in particular its article 11;

Adopts the following guidelines on data protection impact assessments:

The General Data Protection Regulation (GDPR) promotes the principle of accountability of organizations, the concrete implementation of which is based in particular on the performance of impact analyzes relating to data protection (AIPD or Privacy Impact Assessment - PIA). ) for processing likely to create a high risk for the rights and freedoms of individuals.

In introductory remarks, the National Commission for Computing and Liberties recalls the importance of the DPIAs which, beyond their mandatory nature in certain cases and the penalties incurred in the event of breach of this obligation, allow each data controller concerned to identify the guarantees necessary to ensure and demonstrate the compliance of the processing it plans to implement with regard to the requirements of the GDPR. The DPIAs are above all an opportunity to carry out internal reflection, specific to each processing operation, such as to operationally guarantee compliance with the principles relating to data protection and to be able to demonstrate it, if necessary.

The commission therefore wanted to support data controllers in this essential process by offering them various tools such as methodological guides as well as software to help with the drafting of DPIAs, available on its website.

In addition to those adopted on October 4, 2017 at European level by the Article 29 Working Party (G29), and endorsed by the European Data Protection Board (EDPS) on May 25, 2018, the Commission also considered useful to adopt guidelines in order to specify the scope of the obligation to carry out a DPIA, the conditions for carrying it out and, finally, the cases in which a DPIA must be sent to him.

The data controllers concerned by the performance of a DPIA may also refer to the sectoral reference systems that the Commission has adopted in order, on the one hand, to assess the necessity and the proportionality of the processing operations envisaged or implemented and, on the other hand, to identify the guarantees that must be provided to protect the

rights and freedoms of the persons whose data will be processed. These standards can usefully enlighten data controllers on the commission's expectations.

The commission may also, in certain cases, give these standards legal effect, by exonerating from the performance of the DPIA those responsible for processing who strictly comply with them. Each benchmark will specify the effects attached to it (benchmark serving as a simple aid for drafting the AIPD; benchmark allowing exemption from the production of a AIPD).

1. Scope of processing subject, or not, to the performance of a DPIA

1.1. Processing subject to the performance of a DPIA

Article 35.1 of the GDPR provides that the controller must carry out a DPIA when processing is likely to create a high risk for the rights and freedoms of natural persons.

- The regulation itself gives three types of processing likely to present a high risk:

- the systematic and in-depth evaluation of personal aspects based on automated processing and on the basis of which decisions are taken which produce legal effects with regard to a natural person or significantly affect him in a similar way;

- large-scale processing of sensitive data or data relating to criminal convictions and offences;

- systematic large-scale monitoring of an area accessible to the public.

- In addition to these three processing operations, the EDPS has identified nine criteria making it possible to characterize a processing operation likely to generate a high risk:

- data processed on a large scale;

- sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or health data, biometric data and data concerning life or sexual orientation) or data of a highly personal nature (data relating to electronic communications, location data, financial data, etc.);

- data concerning vulnerable people (patients, elderly people, children, etc.);

- crossing or combination of data;

- evaluation/scoring (including profiling);

- automated decision-making with legal or similar effect;

- systematic monitoring of people;

- processing that may exclude the benefit of a right, service or contract;

- innovative use or application of new technological or organizational solutions.

The committee generally considers that processing which meets at least two of the criteria mentioned above must be subject to DPIA.

However, it will be possible to deviate from the above recommendation in certain cases. A controller who considers that his processing, although meeting two of the criteria mentioned above, does not in fact present a high risk, should explain and document his decision not to carry out a DPIA including, if he has been appointed , the opinion of the Data Protection Officer (DPO). Conversely, a manager may consider that his processing presents a high risk even though he meets only one of the above criteria. As a result, he will perform a DPIA.

The committee considers that in case of doubt, a DPIA should be carried out.

- Finally, the GDPR requires the supervisory authorities to draw up a list of processing operations for which a DPIA is required (article 35.4).

This list was drawn up by the Commission as part of its deliberation no. 2018-327 of October 11, 2018 relating to the types of processing operations for which a data protection impact analysis is required, after taking account of the opinion issued by the EDPS on 25 September 2018; this list is called upon to be regularly reviewed by the commission according to its assessment of the high risks that certain treatments may present.

1.2. Processing not subject to AIPD

In general, processing that is not likely to create a high risk for the rights and freedoms of natural persons is not subject to the DPIA.

- The GDPR authorizes national data protection authorities to adopt a list of processing operations which do not have to be preceded by a DPIA (article 35.5).

On this basis, the commission will establish a list of processing operations which, in any event, do not present a high risk and are therefore not subject to the performance of a DPIA. Here too, this list will be regularly reviewed by the committee.

- Unless otherwise provided by law, processing that meets a legal obligation to which the data controller is subject, or necessary for the performance of a public service mission entrusted to the data controller, is also not subject to DPIA. processing, when this processing has a legal basis in national or European Union law, that this law regulates it, and that a DPIA has already been carried out when this legal basis is adopted.

The committee considers that this possibility should be widely used by the public authorities, given its scope and the assistance it will provide to the data controllers concerned.

- A DPIA is also not required when the nature, scope, context and purposes of the processing operations envisaged are very similar to processing for which a DPIA has already been carried out by the controller or by a third party (authorities or public bodies, group of data controllers, etc.); in this case, the results of the DPIA already carried out can be reused.

However, in the case of a DPIA carried out by a third party, the data controller concerned must transpose, in whole or in part, the results of the DPIA to his particular situation.

The commission recalls that, however, processing not subject to AIPD must comply with the data protection principles referred to in Article 5 of the GDPR and the rights of the persons concerned. The commission has drawn up sector-based reference frameworks making it possible to provide guarantees to ensure compliance with the GDPR to which the data controllers concerned may refer, if necessary.

1.3. Special cases of processing implemented before the entry into force of the GDPR

The commission considers that the processing regularly implemented before May 25, 2018 - that is to say having been the subject of a formality with the CNIL, having been exempted from it, having been authorized by a regulatory act or yet having been registered in the register of a data protection officer (CIL) - do not have to be the subject of a DPIA within three years from 25 May 2018, unless they have been substantially modified since their implementation.

2. Conditions for carrying out a DPIA

A DPIA must be carried out before the implementation of a processing operation presenting a high risk for the rights and freedoms of the natural persons concerned; it must be reviewed on a regular basis, in any event every three years, to ensure that the level of risk remains acceptable. One and the same DPIA can relate to a set of similar processing operations in terms of nature, scope, context, purpose and risks presented for the rights and freedoms of the persons concerned.

Article 35.7 of the GDPR sets out the minimum content of a DPIA:

- a systematic description of the planned processing operations and their purposes
- an assessment of the necessity and proportionality of the processing operations with regard to the purposes;
- an assessment of the risks to the rights and freedoms of the data subjects, and
- the measures envisaged to deal with the risks.

Whatever the method chosen by the data controller, the commission considers that it must meet the criteria set out by the EDPS in its guidelines of 4 October 2017 (acceptability criteria for a DPIA).

A DPIA must be carried out by the data controller concerned, or under his authority.

The commission recalls that the realization of a DPIA must involve all the parties involved in the processing in question. This concerns, where applicable, and in a non-exhaustive manner:

- the data protection officer (DPO) whose advice must be requested and formalized in the AIPD and the information systems security officer (RSSI);
- the subcontractor(s) concerned who have an obligation to cooperate;
- the persons concerned by the processing or their representatives, whose consultation may, in certain cases, be relevant to assess the risks;
- project management and project management depending on the context.

The commission recommends documenting the contributions of each stakeholder solicited or, conversely, the choice made not to collect the opinion of a given stakeholder.

Finally, the commission considers that a data controller who has carried out a DPIA can usefully produce a report or a summary intended to be published in order to create a climate of trust and transparency between the parties concerned by the processing.

3. Obligations to send a AIPD to the CNIL

A DPIA showing high residual risks despite the measures envisaged by the data controller concerned must be sent to the CNIL under the conditions provided for in Article 36 of the GDPR.

The data controller may, if necessary, rely on the sectoral reference systems issued by the CNIL: compliance with a reference system will make it possible to consider that there are no high residual risks while the processing is carried out should lead the data controller concerned to, at the very least, question the level of residual risk that may require mandatory consultation of the commission.

Finally, the committee considers that a DPIA relating to a processing project covered by Article 54 III of the Data Protection Act (processing of personal data in the field of health) must be sent to it in the context of the instruction of the request for authorization of which it is seized.

In any case, the commission recalls that the AIPD may, pursuant to articles 58 of the GDPR and 44 of the law of January 6, 1978, be requested from the data controllers concerned, in particular within the framework of the investigation of complaints whose it would be seized or within the framework of the control of the implementation of the treatments.

The president

I. Falque-Pierrotin