Towards a method for data protection impact assessment: Making sense of GDPR requirements

Kloza, Dariusz; Van Dijk, Niels; Casiraghi, Simone; Vazquez Maymir, Sergi; Roda, Sara; Tanas, Alessia; Konstantinou, Ioulia

Published in:
d.pia.lab Policy Brief

DOI:
10.31228/osf.io/es8bm
10.5281/zenodo.5121534

Publication date:
2019

Document Version:
Final published version

Towards a method for data protection impact assessment: Making sense of GDPR requirements

d.pia.lab Policy Brief No. 1/2019

Dariusz KLOZA, Niels VAN DIJK, Simone CASIRAGHI, Sergi VAZQUEZ MAYMIR, Sara RODA, Alessia TANAS and Ioulia KONSTANTINOU

Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)

This policy brief lays the foundations for a method for data protection impact assessment (DPIA) in the European Union (EU). First, as a prerequisite, it proposes a generic method for impact assessment, which is intended to be used – when tailored to the particular context – in multiple domains of practice, such as environment, technology development or regulation (Section 2). Next, building on this generic method and interpreting the requirements of the General Data Protection Regulation (GDPR), this policy brief lays the foundations for a specific method for the process of DPIA in the EU, which is also intended to be adapted to the context of use (Section 3). In particular, the policy brief aims to clarify two crucial aspects of this specific method, which have thus far proved to be the most contentious. These aspects are the appraisal techniques (that is, the necessity and proportionality assessment, and risk appraisal), and stakeholder involvement (including public participation) in decision-making. Section 4 summarises the findings and calls for further guidance, clarification and tailoring down. This policy brief is addressed predominantly to policy-makers who develop methods for impact assessment, practitioners who tailor these methods to the context in which they are used and assessors who conduct the assessment process in accordance with these methods.

1 INTRODUCTION

1.1 CONTEXT

The General Data Protection Regulation (GDPR, or the Regulation) is the core instrument of the reformed legal framework for personal data protection in the European Union (EU). The Regulation brings to the fore a plethora of new solutions whose aim, *inter alia*, is to ensure the 'consistent and high level of protection of natural persons' (Recital 10) whenever their personal data are being processed. Amongst these novelties is an obligation for a data controller to conduct the process of data protection impact assessment (DPIA) before starting to process personal data. This process is required whenever the envisaged data processing operations are likely to result in a 'high risk to the rights and freedoms of natural persons' (Article 35(1)), and it is done to 'ensure the protection of personal data and to demonstrate compliance' with the law (Article 35(7)(d)).

DPIA constitutes a form of impact assessment (IA) and – to a large extent – is a variation of privacy impact assessment (PIA). Generally speaking, impact assessment is an evaluation technique used to analyse the possible consequences of an initiative for a relevant societal concern or concerns (i.e. a matter or matters of interest or importance), if this initiative could present danger to these concerns, with a view to supporting an informed decision on whether to deploy the initiative and under what conditions, and it constitutes – in the first place – a means to protect those concerns.

The obligation to conduct DPIA reflects the risk-based approach to the protection of personal data in the reformed EU legal framework and the strengthening of the principle of accountability therein (Article 5(2)). Drawing on the experience of evaluation techniques in other domains of practice (e.g. environmental, technology or regulatory impact assessment), it is expected that DPIA could become a powerful vehicle for compliance with, and enforcement of, personal data protection (law).

At the same time, the process of DPIA is being progressively mandated in other instruments in the EU legal framework for personal data protection. Besides the GDPR, a legally binding obligation to conduct the process of DPIA is, so far, present in Directive 2016/680 on the protection of personal data in criminal matters (Article 27), in Regulation 2018/1725 on the protection of personal data processed by Union institutions, bodies, offices and agencies (Articles 39 and 89), and in Directive 2019/1024 on open data and the re-use of public sector information (Recital 53). The proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation), if adopted in its current wording, would also require a process of DPIA to be conducted in certain situations (Article 6). (Earlier, the EU experimented with voluntary frameworks for PIA and DPIA for radio-frequency identification (RFID) and 'smart' energy grids.) In parallel, the Council of Europe's modernised 'Convention 108' gave a legal mandate for a comparable obligation (Article 10(2)). Beyond Europe, various forms of PIA and DPIA have been practised in Australia, Canada, Japan, South Africa, South Korea, the United States and New Zealand, among other countries. At the same time, international organisations, such as the International Committee of the Red Cross, require such an assessment process in their by-laws.

 | ISSN 2565-9936

These legally binding obligations to conduct the process of DPIA in the EU raise a number of questions due to, for example, key new concepts on which DPIA is built (e.g. a risk to a right), occasional vagueness in the terminology used in the legal instruments (e.g. 'large scale' or 'systematic'), and rather high fines for non-compliance and malpractice. Furthermore, the stipulation of only the key aspects of DPIA gives a great deal of flexibility at the expense of legal certainty, hence requiring interpretation and normative guidance. (The European Commission, when tabling the proposal for the reform of the legal framework for personal data protection, termed this approach the 'legal hook', and indicated that the legislator should spell out only the minimum of the elements that are deemed essential. Any further specification, if necessary, was expected to come from the relevant industry or governance sectors, for example. Only if these efforts failed or were insufficient was the legislator supposed to intervene.) In 2017, the then-Article 29 Working Party issued high-level guidelines on DPIA in the EU and on determining whether a data processing operation is 'likely to result in a high risk'. The guidelines clarified some aspects pertaining both to the framework and to the method (e.g. threshold analysis) of impact assessment, yet treated some aspects superficially (e.g. the necessity and proportionality assessment or stakeholder involvement). Academic and professional guidance has not yet offered much clarification, either. One of the aspects concerns the method, that is, the set of steps for conducting the assessment process, and the present policy brief is devoted thereto.

1.2 BACKGROUND

The 'architecture' for impact assessment typically consists of two main elements, the 'framework' and the 'method'. A *framework* constitutes an 'essential supporting structure' or organisational arrangement for something, which, in this context, concerns the policy for impact assessment, and defines and describes the conditions and principles thereof. In turn, a *method*, which is a 'particular procedure for accomplishing or approaching something', concerns the practice of impact assessment and defines the consecutive and/or iterative steps to be undertaken to perform such a process. A method corresponds to a framework and can be seen as a practical reflection thereof. This 'architecture' is often supplemented by *guidelines* (handbooks, manuals) and *templates*, which further explain the assessment process and assist with structuring the entire process and drafting a final statement (a *report*) to document it.

Multiple frameworks and methods for impact assessment already exist, in many domains of practice and with varying applicability and quality. A constant need for new ones is a function of the principle of receptiveness of impact assessment, that is, both the framework and the method are to be continuously improved if impact assessment is to serve its goals better (by learning from its own experience or the experience of other evaluation techniques), to respond better to societal change, and to give effect to new domains of practice for impact assessment (e.g. a recently proposed 'algorithmic impact assessment').

1.3 STRUCTURE

In this policy brief, the d.pia.lab lays the foundations for a specific method for conducting the process of DPIA in the EU. As a prerequisite, it proposes a generic method for impact assessment, which is intended to be used – once it is tailored for the particular context (e.g. the industry or governance sector) – in multiple domains of practice, such as environment, technology development or regulation (Section 2).

The generic method reflects a 16-principle framework for impact assessment in multiple domains of practice, developed in the d.pia.lab's previous policy brief (2017). The second method is specific to the domain of personal data protection and – more concretely – concerns the process of DPIA in the EU. It is interpreted from the provisions of the GDPR in the light of the generic method (Section 3). This method also needs to be adjusted to the context of use. In constructing the latter method, the d.pia.lab has focused on particularly contentious issues, such as stakeholder involvement (including public participation) in decision-making, and under-debated issues that have thus far proved to be difficult in practice, such as the necessity and proportionality assessment, and the assessment of the risk to the rights and freedoms of individuals. These two methods are built on a critical appraisal and comparative analysis of the existing frameworks and methods for impact assessment, and the experience of these in various domains of practice, in particular privacy, personal data protection (informational privacy), technology development, environment, regulation and human rights.

This policy brief has two main addressees. Since methods for impact assessment need to be adapted to the context of use, the first addressees are policy-makers, particularly data protection authorities (DPAs) at EU and Member State levels, who need to develop methods for DPIA that are adjusted to their national contexts. This policy brief is also addressed to the stakeholders who tailor these DPIA methods for a particular context of use and – eventually – to data controllers conducting the assessment process. At the same time, the generic method for impact assessment is similarly expected to be of use in multiple domains where impact assessment is practised.

2 A GENERIC METHOD FOR IMPACT ASSESSMENT

The proposed generic method for impact assessment was built on a comparative analysis and a critique of the recurring steps in assessment methods practised in multiple domains, refined with d.pia.lab's own experience. In parallel, the generic method reflects the 16-principle framework offered in d.pia.lab's 2017 policy brief.

The generic method lays the foundations for specific methods for impact assessment in multiple practice domains. The generic method consists of ten steps (six consecutive steps, three steps executed throughout the entire process and one step conducted afterwards), grouped into five phases. Some of these steps follow a logical sequence, while others are a function of the principles embodied in the framework. These steps are the following:

Phase I: Preparation of the assessment process

1) *Screening (threshold analysis)*. This step determines whether the process of impact assessment is warranted or necessary for a planned initiative or a set of similar initiatives, in a given context. The screening is based on an initial yet sufficiently detailed description of the said initiative, both contextual and technical. The determination is made in accordance with

threshold criteria, both internal (i.e. the organisation's own policies) and external (i.e. those set out in legal or other regulatory requirements), or *ad hoc* criteria, such as public pressure. If an assessment process is neither warranted nor necessary, the entire process is then concluded with a reasoned statement of no significant impact.

2) *Scoping*. This step, based on the initial description, is taken to identify:
   a) a societal concern, or concerns, that may be touched on by a planned initiative, such as privacy, personal data protection, (applied) ethics, or the natural and human (biophysical) environment, and the corresponding legal or other regulatory requirements; these concerns will constitute a benchmark of the assessment process;
   b) stakeholders who might affect, be affected by, be concerned with or be interested in the envisaged initiative(s), or who possess knowledge thereof, as well as the level of their involvement;
   c) techniques (methods *sensu stricto*) for the appraisal of impacts and for stakeholder involvement, including public participation, in decision-making, which will be used throughout the assessment process; and
   d) other evaluation techniques, beyond the process of impact assessment, which might be necessary or warranted in order to ensure, for example, the completeness of the information used in the decision-making process (e.g. technology assessment or environmental impact assessment).

   Not all of these elements and people might be identifiable at the beginning of the assessment process, and hence their identification might need to be revised periodically.

3) *Planning and preparation*. This step defines the terms of reference for the performance of the assessment process. These terms include, among others:
   a) the objectives thereof;
   b) the criteria for the acceptability of negative impacts;
   c) the necessary resources (i.e. time, money, workforce, knowledge, know-how, premises and infrastructure);
   d) the procedures and time-frames for the assessment process;
   e) the assessor or the team of assessors (in-house or outsourced), their roles and responsibilities, and assurance of their professional independence; and
   f) the continuity of the assessment process.

Phase II: Assessment

4) *Description*. This step, based on the initial description (cf. Step 1), provides a detailed, two-part account of the planned initiative. First, there is a *contextual description*, which typically consists of:
   a) an overview of the planned initiative(s) and of the sponsoring organisation;
   b) the context of deployment of the initiative;
   c) the need for the initiative;
   d) possible interference(s) with societal concern(s); and
   e) the expected benefits and drawbacks.

   Second, there is a *technical description.* In the case of environmental impact assessment (EIA), this gives an account of, for example, the affected components of the biophysical environment, and, in the case of DPIA, it describes, for example, the categories of personal data and their flows within a processing operation.

5) *Appraisal of impacts*. In this step, the impacts of the envisaged initiative are appraised in accordance with the pre-selected techniques. These impacts pertain to the societal concern(s) that might be touched on by the planned initiative, and to the stakeholders who are largely external to the sponsoring organisation. Typically, this appraisal consists of – at least – a detailed identification, analysis and evaluation of the impacts. The appraisal techniques could range from risk analysis (qualitative or quantitative risk management, or a combination of the two), scenario analysis (planning) and technology foresight to a legal and regulatory compliance check, legal interpretation techniques, and a proportionality and necessity assessment, to a cost-benefit analysis (CBA) and a strengths, weaknesses, opportunities and threats (SWOT) analysis.

Phase III: Recommendations

6) *Recommendations*. In this step, concrete, detailed measures (controls, safeguards, solutions, etc.), their addressees, their priorities and the time-frames for addressing them are proposed to minimise the negative impacts of the planned initiative and, if possible, to maximise the positive ones. The assessor justifies her distinction between 'negative' and 'positive' impacts, since this distinction is contextual and subjective. The assessor takes stock of the measures already implemented. On this basis, after the conclusion of the assessment, the leadership of the sponsoring organisation takes a decision as to the deployment of the initiative and the conditions therefor. (However, a sponsoring organisation might implement the recommendations progressively, still within the assessment process.) An initiative is normally cancelled altogether if the negative impacts are unacceptable; to carry out such an initiative would be exceptional and would require sufficient justification.

Phase IV: Ongoing steps

7) *Stakeholder involvement, including public participation, in decision-making*. This is an ongoing, cross-cutting step that runs throughout the entire process, in which stakeholders, including the public and/or their representatives, take part in the assessment process.

   Understood broadly, a stakeholder is someone who holds a stake (interest) in something, regardless of whether or not he or she is aware of this and of whether the interest is articulated directly or not. In the context of impact assessment, it is someone who is (now) or might be (in the future) affecting, or who is (might be) affected by, concerned with or interested in a planned initiative, (potentially) positively and/or negatively. At the same time, a stakeholder can be someone who possesses specific knowledge and know-how about the initiative, that is, an expert. The concept of a stakeholder is therefore open-ended and comprises the public (laypeople, etc.), decision-makers, experts, and so on. Stakeholders can be individuals

or collective entities, regardless of whether they are formally (legally) recognised or not (and so may be societal groups, communities, nations, the public at large, civil society organisations, etc.). There are multiple (groups of) stakeholders and hence they can be grouped into internal (e.g. employees, work committees) and external ones (e.g. customers or non-governmental organisations), and primary (i.e. those with a direct stake in the initiative, e.g. investors) and secondary ones (i.e. those with an indirect interest yet influential, e.g. the state), or they can be classified by their attributes: power, legitimacy and urgency.

Stakeholder involvement constitutes an integral component of the assessment process and normally it is omitted only in exceptional situations. If stakeholder involvement is neither warranted nor necessary, this choice is reasoned and documented. Whenever stakeholder involvement is mandatory, legal remedies are available for the entitled stakeholders if their involvement is absent or insufficient, commensurate with the level of involvement pursued in a given assessment process. In any case, stakeholder involvement does not compromise any legitimate secrecy (e.g. state or trade secrets), nor it brings any negative consequences for its participants (e.g. exploitation).

The level of stakeholder involvement can range from: (a) merely being informed or taught about a planned initiative (low level); to (b) dialogue and consultation, in which the stakeholders' views are sought and taken into consideration (middle level); or even (c) the co-decision by the stakeholders and a sponsoring organisation about the deployment of the initiative in question and, subsequently, partnership with the stakeholders in its implementation (high level).

There are a plethora of techniques for stakeholder involvement, ranging from information notices to interviews, questionnaires and surveys, to focus groups, roundtables, workshops and citizens' panels, and including structured techniques, such as a 'world café' or 'Delphi'. An appropriate technique, or a combination of techniques, is selected depending on the level of stakeholder involvement desired, the planned initiative, the context of the deployment of the initiative and the resources at the disposal of the sponsoring organisation.

Stakeholder involvement can bring several benefits to the assessment process (e.g. enhancing its quality, credibility and legitimacy) and to the outcome (e.g. the decision-making process being better informed), but these must be contrasted with its drawbacks, which include the question of representativeness (over- or under-representation), fairness (e.g. manipulation, 'astroturfing'), reluctance, communication barriers, conflict between public and private interests, and the resource-intensive nature of the entire stakeholder involvement process.

8) *Documentation*. This is an ongoing, cross-cutting step that runs throughout the entire process, in which intelligible records are kept, in writing or in other permanent form, of all the activities undertaken during the assessment process. This step includes the preparation of a final report from the assessment process (or a statement of no significant impact, when applicable). The full spectrum of documentation from a given assessment process, preferably in an electronic format, might be made publicly available, centrally registered, and/or presented for inspection upon request (with due respect for legitimate confidentiality).

9) *Quality control*. This is an ongoing, cross-cutting step that runs throughout the entire process, in which the adherence to a standard of performance is checked, either internally (e.g. through progress monitoring or a review by the sponsoring organisation) or externally (e.g. by an independent regulatory authority through an audit, or by a court of law), or both. The quality control can equally well occur during or after the assessment process, or in both.

Phase V: Revisiting

10) *Revisiting*. In this step a decision is made as to whether to conduct the process again, entirely or in part. This step can occur every time the envisaged initiative is modified (before or after its deployment) or every time the context in which it is going to be deployed, or already has been deployed, changes. This step also ensures the continuity of the assessment process, such as in the case of a transfer of the initiative to another organisation.

The above-mentioned method for assessing the impacts of an initiative on a societal concern, or concerns, is of a generic nature and needs to be tailored down to the specificity and needs of a given domain of practice, of the stakeholders (including the public) involved, and of the context of use. For example, assessing the impacts in the domain of personal data protection in the EU implies a specific approach, at least, during the *Screening* (threshold criteria), *Scoping* (e.g. a list of societal concerns), *Appraisal of impacts* (e.g. techniques for the appraisal and a list of possible impacts), *Stakeholder involvement, including public participation, in decision-making* (e.g. stakeholders and techniques for involving them) and *Recommendations* steps.

RELEVANT GDPR PROVISIONS

Article 35

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. […]
7. The assessment shall contain at least:
   a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
   b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   c) an assessment of the risks to the rights and freedoms of data subjects […]; and
   d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. […]

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Article 36

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment […] indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing […] would infringe [the] Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall […] provide written advice to the controller and, where applicable to the processor, and may use any of its powers […].

3 A METHOD FOR DATA PROTECTION IMPACT ASSESSMENT IN THE EUROPEAN UNION

The specific method for DPIA required by the GDPR in the EU and described below was interpreted on the basis of the densely formulated provisions of Articles 35-36 and in the light of the generic method. The GDPR obliges a data controller to conduct the assessment process, and a data processor, if applicable, to assist the data controller. It is the data controller who is held accountable for the assessment process.

The Regulation foresees seven steps to be undertaken, namely:

1) *Screening (threshold analysis)*: in order to determine whether a process of DPIA is required by law, the data processing operations envisaged, on the basis of an initial description of these operations and of a rudimentary risk appraisal, have to be examined against the following six criteria:
   - *Criterion 1 – likelihood of high risk (general)*: at the most general level, the Regulation requires a process of DPIA to be conducted for processing operations likely to present a high risk to the rights and freedoms of natural persons, taking into account four qualitative criteria – the nature, the scope, the context and the purposes of the processing of personal data. In particular, data processing operations involving new technologies constitute a specific trigger for the assessment process (Article 35(1)). These criteria, however, are not further defined. They could include, for example, the processing of special categories of personal data, data relating to criminal convictions and offences, data related to security measures or biometric data (i.e. the nature of the processing operations), the amount of data processed, the geographical reach and the number of people affected (i.e. the scope), the use of a given type of technology or the area of use (e.g. publicly accessible) (i.e. the context), or data for profiling or automated decision-making (i.e. the purpose) (cf. Recital 91). The then-Article 29 Working Party, in its opinion on how to determine whether processing is 'likely to result in a high risk' (2017), advised that nine criteria should be considered when determining whether the risk is at a high level; examples of the criteria are whether datasets are being matched or combined, and whether the processing of personal data concerns vulnerable data subjects. Nonetheless, it is for the data controller to determine whether the level of risk is high.
   - *Criterion 2 – likelihood of high risk (enumeration)*: the Regulation foresees three types of data processing operations for which a DPIA is required because such operations are likely to present a high risk to the rights and freedoms of natural persons. In other words, the following data processing operations are deemed by law to be highly risky; this list is non-exhaustive:
     - 'systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person';
     - processing, on a large scale, of special categories of data or of personal data relating to criminal convictions and offences; and
     - 'systematic monitoring of a publicly accessible area on a large scale' (Article 35(3)).
   - *Criterion 3 – likelihood of high risk (positive enumeration by data protection authorities)*: a national or regional data protection authority (DPA) is entitled to determine, for its own jurisdiction, further types of data processing operations for which a process of DPIA is required (Article 35(4)).
   - *Criterion 4 – likelihood of high risk (negative enumeration by DPAs)*: the same authority may determine, for its own jurisdiction, other types of data processing operations for which a process of DPIA is *not* required (Article 35(5)). Both lists, if they involve – generally speaking – cross-border data processing operations, are to be communicated, under the consistency mechanism, to the European Data Protection Board (EDPB) for its opinion (Article 35(4)-(6)). The EDPB has issued such opinions since 2018.
   - *Criterion 5 – previous regulatory impact assessment*: unless Member States decide otherwise, for personal data processed in order to comply with a legal obligation (Article 6(1)(c)) or processed in the public interest (Article 6(1)(e)), on the basis of EU law or the Member State's law, where the processing has already been assessed within some other assessment process in the context of the adoption of that legal basis, the process of DPIA is no longer required, provided this other assessment process essentially satisfies the conditions laid down in the GDPR (Article 35(10)).
   - *Criterion 6 – exemptions for specific professions:* if the processing operations concern 'personal data from patients or clients by an individual physician, other health care professional or lawyer', these operations are not considered to be on a large scale (cf. e.g. Article 35(3)(b)) and hence for such processing operations the process of DPIA is not required (Recital 91).

   If any of the first three criteria is satisfied, a process of DPIA is mandatory. Conversely, if any of the three last criteria is satisfied, the data controller is exempted from conducting the assessment process.

2) *Description*: the Regulation requires the assessment to commence with a 'systematic description of the envisaged processing operations' (Article 35(7)(a)). Such a description includes, in particular:
   a) a *contextual description* of the envisaged data processing operations, particularly their nature, scope, context and purposes, the legitimate interest of the controller (if applicable) and the stakeholders involved (data subjects, controllers, processors, third parties and public authorities);
   b) a *technical description* containing personal data flows and – possibly – a visualisation thereof.

   The description of the envisaged data processing operations can be based on the initial description that was used to determine whether the assessment process was warranted (cf. Step 1).
3) *Appraisal of the envisaged processing operation, or a set of similar operations*: the Regulation requires the use, consecutively or in parallel, of at least two distinct appraisal techniques (methods *sensu stricto*), namely the necessity and proportionality assessment, and risk appraisal. Both techniques constitute, to a large extent, novelties in personal data protection law. Following the 'legal hook' approach, their stipulation in the GDPR is generic and the Regulation does not specify how exactly these techniques are to be used.
   a) The assessment of the 'necessity and proportionality of the processing operations in relation to [their] purposes' (Article 35(7)(b)).

      The necessity and proportionality assessment refers to the observance of the personal data protection principles (Article 5(1)). In particular, it concerns the principle of purpose limitation – that is, it first asks about the purpose of the data processing operation, whether 'the processing could not reasonably be fulfilled by other means' (Recital 39) and whether the personal data would be 'collected for specified, explicit and legitimate purposes and not further processed' in a way that is inconsistent with those purposes (Article 5(1)(b)). This assessment further concerns the principle of lawfulness of processing (Article 6), and the principles of data minimisation, accuracy and storage limitation. In other words, it asks whether the personal data would be 'processed lawfully, fairly and in a transparent manner', would be 'adequate, relevant and limited to what is necessary in relation to the purposes', would be 'accurate and, where necessary, kept up to date' and would be stored for no longer than necessary (Articles 5(1)(a)-(e)).

      This assessment is made on a fact-based analysis, built on sufficient, clearly described and verifiable evidence. The content of the necessity and proportionality assessment differs between the private sector and the public sector. In addition, for the latter sector further differentiation is needed between law-making and law-applying.
   b) The assessment of the 'risks to the rights and freedoms of data subjects' (Article 35(7)(c)).

      Risk assessment, in the context of DPIA, typically refers to a detailed identification, analysis and evaluation of the possible future negative consequences of data processing operations, and, more concretely, to the harms caused by such operations. Their assessment pertains to 'physical, material or non-material damage' and includes, for example, discrimination, identity theft or fraud, financial loss or damage to reputation, loss of confidentiality, unauthorised reversal of pseudonymisation, any significant economic or social disadvantage, loss of control over personal data, and processing of unauthorised sensitive data or data from vulnerable natural persons, in particular children (Recital 75 provides a longer list of examples of such harms; their further identification occurs during the assessment process). The decision on whether a processing operation involves a risk and – subsequently – whether the level of risk is high is made by the data controller and is made 'on the basis of objective assessment' (Recital 76).

      The risks to be assessed in the process of DPIA relate to natural persons, including data subjects and society at large, and not to data controllers or processors. These risks concern the enjoyment of rights and freedoms by individuals and therefore they are not (merely) compliance risks. Given the goal of the Regulation, these risks have a wider scope than solely the right to the protection of personal data and extend to other rights and freedoms in an open-ended way. (Recital 4 indicates rights such as privacy, effective remedy, fair trial, and cultural, religious and linguistic diversity, and freedoms such as freedom of thought, conscience and religion, freedom of expression and information, and freedom to conduct a business.)

      Risks to the rights and freedoms are largely appraised qualitatively, by evaluating their severity (the magnitude of the risk) and likelihood (feasibility of occurrence, e.g. low, medium or high), measured by reference to the 'origin', 'particularity' (Recital 84) and 'nature, scope, context and purposes of processing' (Recitals 75-76). Certain data protection risks, such as data security risks, could be appraised quantitatively (e.g. by calculating their severity and probability). The appraisal of risks can be based on the initial appraisal that is used to determine if the assessment process is warranted (cf. Step 1).
4) *Stakeholder involvement (public participation) in decision-making*: the Regulation foresees, 'where appropriate', consultation with data subjects or their representatives, with due respect for legitimate secrecy (i.e. the 'protection of commercial or public interests or the security of processing operations') (Article 35(9)). The 'appropriateness' of a consultation is not to be understood as meaning a consultation is 'optional'. Exceptions can be made if, for example, no new insight could be gained by the involvement of stakeholders, or it would require an effort that would be disproportionate to the results. A decision not to involve stakeholders, or to deviate from the results of such a consultation, is reasoned and documented. In parallel, a data protection officer (DPO), if designated and upon request, is to be consulted and to provide advice (Articles 35(2) and 39(1)(c)); nevertheless, the DPO *cannot* conduct the assessment process.
5) *Recommendations*: the Regulation requires the assessment process to be concluded with a list of recommended measures envisaged to:
   a) address the risks, 'including safeguards, security measures and mechanisms to ensure the protection of personal data', and
   b) ensure compliance with the Regulation, 'taking into account the rights and legitimate interests of data subjects and other persons concerned' (Article 35(7)(d)).

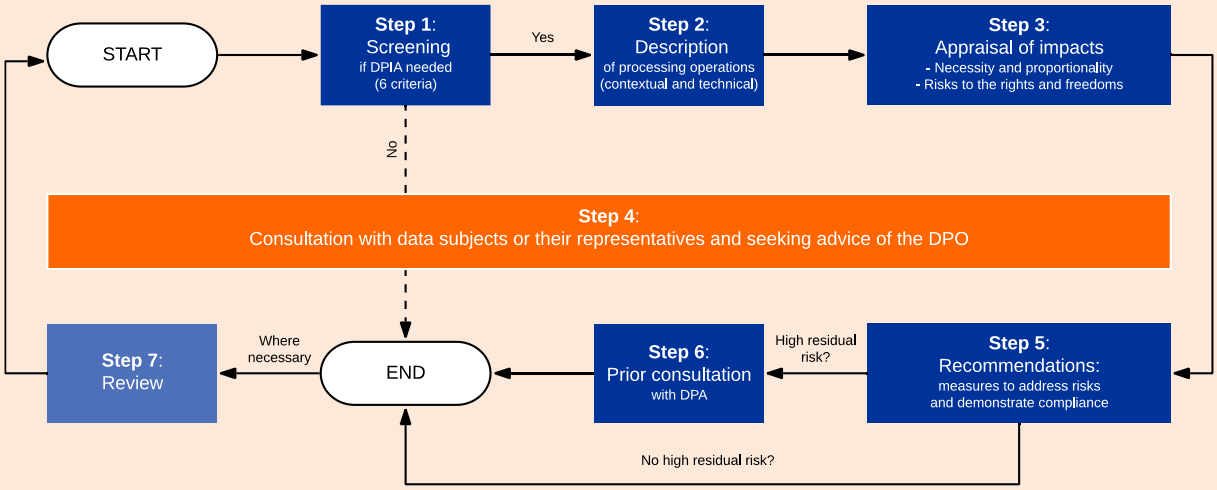
The outcome of the assessment process is to be 'taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with [the] Regulation' (Recital 84).

6) *Prior consultation with a supervisory authority*: the Regulation links the process of DPIA with prior consultation. In case of a high residual risk, that is, when the assessment process demonstrates a risk of a high level that would remain even after the data controller implemented the recommendations stemming from the assessment process, the data controller is obliged to refer to a DPA for consultation, prior to the start of the personal data processing and in accordance with a prescribed procedure (Article 36).

7) *Review*: when 'necessary', 'the controller shall carry out a review to assess if the processing is performed in accordance with the [DPIA] at least when there is a change of the risk represented by processing operations' (Article 35(11)). This review can therefore occur merely after a certain period of time, for monitoring purposes, or when there is a change that renders the previous assessment obsolete (partially or totally). However, the Regulation does not stipulate the consequences of such a review; given the possibility of a change of risk, the assessment process might need to be conducted again (in part or entirely).

The specific method for DPIA proposed above lays the foundations for the adjustment of this method to match a given context of use, such as in telecommunications or 'smart' energy grids, while ensuring the 'protection of personal data' and demonstrating 'compliance with [the] Regulation' (Article 35(7)(d)).

THE PROCESS OF DPIA AS INTERPRETED FROM ARTICLES 35-36 GDPR



According to this interpretation, the GDPR does not fully address all ten steps of the generic method. Some steps do not necessarily merit being regulated by the law, but they emerge for pragmatic reasons in the assessment process. In particular, the Regulation does not address the *Scoping* step. (In practice, *Scoping* would, for example, determine what aspects of the right to personal data protection are likely to be affected by an envisaged data processing operation, and who would be a data subject, or the representative of a data subject, of such a processing operation.) Other steps of the generic method can, to a large extent, be interpreted from other provisions in the Regulation. Concerning *Planning and preparation*, the Regulation stipulates only that, for example, a single assessment process might address a set of similar processing operations (Recital 92) or that a data processor is to assist a data controller in conducting the assessment process (Article 28(3)(f)). Concerning *Documentation*, a data controller is, for example, obliged to demonstrate that processing operations are performed in accordance with the law (Article 24(1)). Concerning *Quality control*, for example, a DPO is tasked with monitoring the performance of the assessment process (Article 39(c)) and a DPA is tasked with carrying out audits (Article 58(1)(b)). However, in comparison with the generic method, the GDPR adds the additional step of *Prior consultation with a supervisory authority*.

4 CONCLUDING REMARKS

In the present policy brief, the d.pia.lab lays the foundations for two methods for impact assessment: first, a generic method, reflecting the framework of its previous policy brief and intended to constitute a basis for assessment methods that are tailored down to specific domains of practice and contexts of use; second, a method for DPIA in the EU, based on the generic method and interpreted from the requirements of the GDPR.

The process of DPIA in the EU is built on a number of key new concepts, such as the risk to a right, and – as a consequence of the 'legal hook' approach – this process is rather minimally regulated in the text of the law, and requires interpretation and guidance. Hence, the d.pia.lab has attempted to interpret the method for DPIA from Articles 35-36 GDPR, focusing on under-debated or contentious issues. (Since an obligation to conduct the process of DPIA is present in some EU legal instruments other than the GDPR, these remarks might be applicable thereto *mutatis mutandis*.) Nonetheless, issues such as the techniques for the assessment of necessity and proportionality, for the appraisal of risks to the rights and freedoms of natural persons, and for the involvement of stakeholders, including the public, merit further academic and professional attention, to which the d.pia.lab intends to turn in its future contributions.

At the same time, the method for DPIA interpreted from the requirements of the GDPR still requires further in-depth guidance, clarification and tailoring down. In particular, the EDPB, in concert with national and regional DPAs of the EU, with a view to contributing towards more legal certainty and becoming 'reference centres' for this and other types of impact assessment, is best placed to offer such support. For example, templates for DPIA, adjusted to the circumstances of a given Member State and a given context of use (e.g. industry or governance sector), merit their specific attention.

SELECTED RELEVANT SOURCES

Arnstein, Sherry R. (1969) "A Ladder of Citizen Participation," *Journal of the American Institute of Planners*, 35(4), pp. 216–224. doi: 10.1080/01944366908977225.

De Hert Paul, Dariusz Kloza and David Wright (2012) "Recommendations for a Privacy Impact Assessment Framework for the European Union," Brussels – London. https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf.

Gellert, Raphaël (2018) "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review* 34(2), pp. 279–288. doi: 10.1016/j.clsr.2017.12.003.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," *d.pia.lab Policy Brief* 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

van Dijk Niels, Raphaël Gellert and Kjetil Rommetveit (2016) "A risk to a right? Beyond data protection risk assessments", *Computer Law & Security Review*, 32(2), pp. 286–306. doi: 10.1016/j.clsr.2015.12.017.

Oxford Dictionary of English; https://www.lexico.com/en.

FURTHER READINGS

Article 29 Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev. 01, Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

International Organization for Standardization [ISO] (2018), *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

Jasanoff, Sheila (2012) *Science and Public Reason*. London: Routledge. doi: 10.4324/9780203113820.

European Data Protection Supervisor [EDPS] (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2017) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* [draft]. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

EDPS (2019) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf.

Grunwald, Armin (2018) *Technology Assessment in Practice and Theory*. Abingdon: Routledge. doi: 10.4324/9780429442643.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*. Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Noble, Bram F. (2015) *Introduction to Environmental Impact Assessment. A Guide to Principles and Practice*. Toronto: OUP Canada.

ABOUT D.PIA.LAB

The **Brussels Laboratory for Data Protection & Privacy Impact Assessments**, or **d.pia.lab**, connects basic, methodological and applied research, provides training and delivers policy advice related to impact assessments in the areas of innovation and technology development. Whilst legal aspects of privacy and personal data protection constitute its core focus, the Laboratory includes other disciplines including ethics, philosophy, surveillance studies and science, technology & society (STS) studies. Established in November 2015, the Laboratory constitutes a part of and builds upon the experience of the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB), Belgium.

The Laboratory has built its knowledge base in impact assessments from multiple concluded and on-going research projects such as PERSONA, HR-RECYCLER and SYSTEM (co-funded by the EU) and PARENT (co-funded by Innoviris). The views expressed in this policy brief do not reflect the views of any of the funding agencies.

We thank – in an alphabetical order – Alexandra Aslanidou, Jonas Breuer, Alessandra Calvi, Roger Clarke, Katerina Demetzou, Catherine Jasserand-Breeman, Anna Johnston, Gianclaudio Malgieri, Anna Mościbroda, Kjetil Rommetveit, Julien Rossi, Juraj Sajfert, Laurens Vandercruysse, Heidi Waem, Ine van Zeeland and an anonymous reviewer for their feedback on the earlier draft of the present policy brief.

dpialab.org | **dpialab@vub.ac.be**