Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals

Kloza, Dariusz; Van Dijk, Niels; Gellert, Raphaël Maurice; Borocz, Istvan Mate; Tanas, Alessia; Mantovani, Eugenio; Quinn, Paul

Published in:
d.pia.lab Policy Brief

DOI:
10.31228/osf.io/b68em
10.5281/zenodo.5121575

Publication date:
2017

Document Version:
Final published version

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 No. 1/2017

Dariusz KLOZA, Niels VAN DIJK, Raphaël GELLERT, István BÖRÖCZ,
Alessia TANAS, Eugenio MANTOVANI and Paul QUINN

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

This paper provides recommendations for the European Union (EU) to complement the requirement for data protection impact assessment (DPIA), as set forth in the General Data Protection Regulation (GDPR), with a view of achieving a more robust protection of personal data. In April 2016 the EU concluded the core part of the reform of its legal framework for personal data protection. The Union is currently preparing implementing measures and guidelines to give full effect to the new legal provisions before their applicability from May 2018. This reform introduces, among other 'novelties', a legal requirement to conduct a DPIA. However, this requirement bears a few weak points. In order to remedy that by informing this on-going policy-making process, the present policy brief attempts to draft a best practice for a generic type of impact assessment, i.e. recommended for different areas (section II). Section III makes an early evaluation of how this best practice relates to the specific impact assessment requirement set forth in the GDPR, i.e. DPIA. These sections are preceded by succinct background information on impact assessments as such: definition, historical overview, and their merits and drawbacks (section I). Section IV concludes this paper by offering recommendations for complementing the DPIA requirement in the GDPR: (1) to expand the scope of the DPIA requirement in the GDPR; (2) to develop methods for conducting such an assessment; (3) to establish 'reference centres' on DPIA at data protection authorities (DPAs). This policy brief is addressed predominantly to policy-makers at the EU- and Member State-level, notwithstanding the potential interest it might gain from their counterparts elsewhere in the world.

I. INTRODUCTION

I.1. CONTEXT

The recently reformed personal data protection law in the EU will introduce a requirement for data controllers to conduct an assessment of the impacts of data processing operations that are "*likely to result in a high risk to the rights and freedoms of natural persons*" with regard to the protection of personal data. This new requirement was named the 'data protection impact assessment' and abbreviated 'DPIA', and is expected to play a crucial role in the system of protection of fundamental rights in the EU. Both the relative novelty of this requirement and the fast-approaching applicability of the new law require stakeholders to adapt quickly and have consequently provoked lively debates in the EU and beyond. In particular, policy-makers and DPAs have been interested in the exact shape of a policy for DPIA, while public and private organisations have been focusing on compliance with this new requirement.

I.2. HISTORY

An impact assessment is a tool used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns.

Impact assessments and similar evaluation techniques have grown out of the emergence of new – and, at the time, not fully known – dangers to individual and collective societal concerns. They aim to address uncertainty and risk. For example, technology assessments (TAs) emerged in 1960s in the United States, initially as a tool used by scientists in order to better deal with the potentially dangerous consequences of their discoveries and inventions. They were subsequently institutionalised as a means to ensure – initially – product safety and have progressively encompassed a broader spectrum of issues relating to the society and technology. Likewise, environmental impact assessments (EIAs) surfaced as a response to the gradual degradation of the natural environment. Positive experience with both TAs and EIAs has aided their spread as practice worldwide and has resulted in proliferation, and sometimes institutionalisation, of impact assessments in areas ranging from health care, regulation (governance), national security, surveillance practices to privacy and personal data protection.

The proliferation of privacy- (PIAs) and data protection- impact assessments (DPIAs) is attributed to three main factors: (1) the growing invasiveness of emerging technologies into individual lives and social fabrics, (2) the increasing importance of the processing of personal data for contemporary economy, national security, scientific research and technological development, and inter-personal relations, among others, and (3) the diminishing trust in emerging technologies and the use thereof by public and private organisations. However, some 50 years after impact assessments emerged, they still do not constitute a clear-cut practice. Only in certain areas have they gained considerable experience and matured (e.g. EIA). In other areas, their identities are still being developed (e.g. 'societal' impact assessments or DPIAs) and in other areas, calls for their introduction are constantly being made (e.g. human rights).

PIAs – and subsequently DPIAs – emerged in the 1990s and became institutionalised, in different forms and at various levels of compulsion, first in common law jurisdictions, such as New Zealand, Australia and Canada. In Europe, the earliest policy for PIA was developed in the United Kingdom in 2007. The EU has thus far put in place two sector-specific, voluntary PIA policies: the first for radio-frequency identification (RFID) applications (2009) and the second for 'smart grids' (2012). In the Better Regulation Package (2015), privacy and personal data constitute one of the many objects of assessment in the processes of EU law- and policy-making. After the adoption of both the GDPR and the Police and Criminal Justice Data Protection Directive (2016), a mandatory policy for impact assessment will be first introduced in the EU in May 2018 in the area of personal data protection. This development is not standalone as e.g. the Council of Europe's recently finalised modernisation of 'Convention 108' and the proposed new data protection law in Switzerland (if adopted in its current wording) will both introduce a similar policy.

I.3. MERITS

The merits of impact assessments predominantly lie in their contribution towards (1) informed decision-making and (2) protection of societal concerns. The former category usually attracts public and private organisations, bringing them benefits from a switch to anticipatory, *ex ante* thinking. Those organisations are able to reflect on consequences of their envisaged initiatives as well as on the means to minimise or sometimes even avoid negative and unintended consequences before these occur (i.e. an 'early warning system'), gaining both in resources and public trust. Furthermore, impact assessments can ease compliance with legal and otherwise regulatory requirements (e.g. standards). Being a 'best-efforts obligation', they constitute evidence of due diligence, which can potentially limit or

 | ISSN 2565-9936

even exclude legal liability. They also demonstrate accountability towards regulatory authorities, which in turn have part of their work facilitated. Eventually, impact assessments, if conducted in a transparent manner, appeal to public confidence, showing that an organisation takes societal concerns seriously; the private sector often uses impact assessments to demonstrate corporate social responsibility.

The latter category usually attracts governments because impact assessments help these governments in fulfilling their mission to offer practical and efficient protection of relevant societal concerns (e.g. certain human rights, such as privacy) for the benefit of the individual and the society at large. For individuals, impact assessments are a means to voice their concerns (i.e. through public participation), which enhances procedural justice. Impact assessments seek to accommodate diverse interests and consequently contribute to the drawing of a 'thin red line' between legitimate yet seemingly competing interests, e.g. national security and the protection of personal data (e.g. in DPIA), or the competitiveness of national economy and the protection of natural environment (e.g. in EIA). In comparison with other protection tools, impact assessments provide more scope of protection than e.g. compliance checks, which can often be reduced to mere 'tick box' exercises.

I.4. Drawbacks

Critics have argued that impact assessments constitute an unnecessary burden, adding to already overgrown bureaucracy, causing unnecessary expenditure and delays in decision-making, or even slowing the entire development process (it is thus no surprise that there is a recurrent wish for impact assessments to be quick, simple and cheap). Opponents underline the complexity of the assessment process in practice, the difficulties it brings, along with a lack of practical experience and minimal or non-existent guidance and oversight. They further question their added value over other evaluation techniques, e.g. compliance checks, as well as their efficacy, pointing out the broad discretion often afforded as to whether and how such impact assessments should be conducted.

Impact assessments are often criticised for their seemingly 'lip service' nature, being used solely to comply with a regulatory requirement, for their conduct only with the least amount of effort, or for their instrumental use, being used only to legitimise intrusive initiatives. Moreover, organisations sometimes focus on conducting assessments *in abstracto* instead of using them as a means to address the impact of their envisaged initiatives. They often confuse impact assessments with audits. Organisations inaccurately consider the consequences solely pertaining to themselves (e.g. reputational or financial risks), rather than assessing also the consequences for individuals and the public at large. Ultimately, impact assessments are often performed too late, i.e. when the design of an initiative cannot be meaningfully influenced anymore. Critics further suggest that when impact assessments are compulsory, they represent a regulatory requirement too narrow in its scope, allowing significantly dangerous initiatives to escape scrutiny. When impact assessments have been performed, they usually lack transparency, i.e. the process as a whole is opaque, hard to understand for the layperson (due to a high level of technical complexity) and final results and recommendations are difficult, if not impossible, to find. They often fail to include public participation or give it limited scope, therefore making their participation meaningless.

II. Best practice for impact assessments

Building on a comparative analysis of impact assessments in multiple areas, the authors will now attempt to sketch the elements constituting a best practice for a generic type of impact assessment, i.e. recommended for different areas. This will serve, in the subsequent section, to evaluate the DPIA requirement in the GDPR.

1. The impact assessment is a systematic process, undertaken in accordance with an appropriate method, and conducted in a timely manner. It starts reasonably early in the lifecycle of a single initiative, or a few alike initiatives (e.g. a proposed technology or a piece of legislation), prior to their deployment, continues throughout its life cycle and – as the society changes, dangers evolve and knowledge grows – is revisited when needed (a 'living instrument'), thus continuously influencing the design of the initiative under assessment.
2. Impact assessments analyse possible consequences of an initiative against the relevant societal concerns, both individual and collective, commensurate with its type (e.g. DPIA is about the protection of individuals whenever their personal data are being processed and EIA – natural and human environment). Threshold analysis (scoping, establishing the context), public participation and expert consultation help determining and keeping up-to-date the list of these concerns. Whenever necessary, multiple types of impact assessments are performed for a given initiative, possibly in an integrated way.
3. Not all initiatives require impact assessments. The need is therefore determined by factors such as the nature, scope, context and purpose of the initiative under assessment, the number and types of individuals affected, etc. Impact assessments are however compulsory at least for initiatives capable of causing severe negative consequences to relevant societal concerns.
4. There is no 'silver bullet' method for carrying out impact assessments. What matters is the choice of an appropriate assessment method allowing for the best understanding and treatment of possible consequences of the envisaged initiative. These methods can range from qualitative or quantitative risk management, to scenario planning, to scientific foresight, supported by a compliance check with relevant legal and otherwise regulatory requirements (e.g. technical standards).
5. The impact assessment process not only identifies, describes and analyses possible consequences – positive or negative, intended or unintended – of an initiative under assessment, but also identifies, describes and analyses possible solutions (recommendations) to address these consequences.
6. Impact assessments constitute 'best efforts obligations'. Since it is impossible to reduce negative consequences in absolute terms (and maximise positive ones), organisations react to them to the best of their abilities, depending upon the state-of-the-art and, to a reasonable extent, available resources.
7. The impact assessment process requires the assessor, or a team of assessors, to have sufficient knowledge and know-how for its successful completion, corresponding to the type of impact assessment at stake.
8. The impact assessment process is documented (in particular, in writing) and is reasonably transparent. Its transparency manifests itself in free (i.e. unrestricted) and public access to relevant information. The public at large is informed about the assessment process, its terms of reference (in particular, the method) and its progress. Both draft and final assessment reports are easily accessible. This is without prejudice to legitimate secrecy.
9. The impact assessment process is deliberative, manifested predominantly by public participation. External stakeholders – be it individuals and/or civil society organisations concerned or affected by the initiative under assessment), as representative as possible – are identified and meaningfully informed about it, their voice is actively sought and duly taken into consideration (i.e. consultation and co-decision). Information given and sought is robust, accurate and inclusive. Individuals and/or their representatives have effective means of challenge, e.g. in a court of law or similar tribunal. In parallel, anyone within the organisation sponsoring the initiative under assessment (i.e. internal stakeholders) partakes in the assessment process under the same conditions. Exceptions to public participation, if justified, are interpreted narrowly.
10. An organisation sponsoring an initiative is accountable for the impact assessment process. Decision-makers within an organisation choose, *inter alia*, the method of assessment and assessors to conduct it. They eventually approve the final impact assessment report and subsequently monitor the implementation of proposed possible solutions (recommendations). An external entity (e.g. a regulatory authority or an audit body) scrutinises its quality; selection criteria are transparent. Therefore, an organisation is able to demonstrate the satisfactoriness of the undertaken impact assessment process. Whenever impact assessments are compulsory, non-compliance and malpractice are proportionately sanctioned.
11. The independence of the assessor – be it external or in-house – is ensured: they do not seek nor accept any instructions, and have sufficient resources (i.e. time, money, manpower, knowledge and know-how, premises, and infrastructure) at their disposal.
12. The impact assessment process is sufficiently simple, i.e. not unduly burdensome. The method serves those who use it and

therefore is structured, coherent, easily understandable, and avoids prescriptiveness, over-complication and abuse of resources. There is an inherent trade-off between the simplicity of use, and the technical sophistication and accuracy of the assessment.

13. The impact assessment process is adaptive to the characteristics of an initiative under assessment and its sponsoring organisation (i.e. 'one size does not fit all'), e.g. type and complexity thereof (e.g. technology development, scientific research, legislative proposals) or the type and number of individuals concerned (affected) (e.g. nuclear safety is not the same as personal data protection). It can be connected with impact assessments in other areas, if possible. It is responsive to geographical and cultural differences.

14. The impact assessment process is inclusive. This ensures as many stakeholders, relevant societal concerns and relevant development phases as possible (i.e. both the initiative under assessment and the process leading thereto), commensurate with the societal concerns at stake and the type of assessment, are included in the assessment process. It bases its analysis on both expert and layperson knowledge (i.e. public participation).

15. The impact assessment is receptive. Both the method and the process evolve by learning from previous experience in parallel evaluation techniques (e.g. TA, EIA, risk management, etc.), knowledge from related disciplines (e.g. law), and changes in the society.

16. Impact assessments require a supportive environment to bear fruit. They need continuous high-level support from policy- and decision-makers and a spirit of cooperation among external and internal stakeholders. Regulators offer guidance and practical assistance in the assessment process, in the form of adequate training, guidelines, explanations and advice.

RELEVANT GDPR PROVISIONS

- 'Where a type of processing … is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall … carry out an assessment…' (Art 35.1)
- 'The supervisory authority shall establish … a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment' (Art 35.4)
- 'The assessment shall contain at least … measures envisaged to address the risks … taking into account the rights and legitimate interests of data subjects and other persons concerned' (Art 35.7.d)
- 'Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing …' (Art 35.9)
- 'Infringements [… shall be] subject to administrative fines up to 10 000 000 EUR…' (Art 83.4)

III. EVALUATION OF THE DPIA REQUIREMENT IN THE GDPR

The authors will now evaluate the specific type of impact assessment, namely DPIA, as set forth in Art 35 GDPR, in light of a best practice for a generic type of impact assessment, as described in the previous section. Particular emphasis will be given to some of the key specificities of the new data protection law in the EU, i.e. the principle of accountability, the 'legal hook' for the DPIA and the 'risk-based approach'.

1. The GDPR, within the scope of its application, makes it compulsory for data controllers, with the help of data processors (if applicable), to conduct a DPIA for certain processing operations "*likely to result in a high risk to the rights and freedoms of natural persons*". A failure to fulfil this requirement is heavily sanctioned. This way the GDPR shifts attention from reactive measures towards more anticipatory ones.

2. By requiring data controllers to carry out a DPIA "*prior to the processing* [of personal data]" and, subsequently, to review their assessments in cases where risks and/or the processing operations have changed, the GDPR implies that the DPIA is a systematic process and a 'living instrument'.

3. The scope of the DPIA requirement follows the scope of the GDPR: it protects the fundamental right to personal data protection as well as other fundamental rights and freedoms affected by the processing of personal data. While the GDPR applies only if such data are being processed, it falls short on safeguarding other relevant societal concerns, arising e.g. from the processing of anonymous data. This way, the scope of protection is not complete.

4. The GDPR requires a DPIA in cases of "*high risk*". This limits its scope to a few types of data processing operations. DPAs are entitled to expand this catalogue yet they can also limit it. Nevertheless, as the GDPR affords a higher level of protection to sensitive personal data and data on criminal records, this was reflected in the scope of the DPIA requirement.

5. The GDPR brings together the concepts of 'risk' and 'right', which traditionally belong to very different spheres of knowledge and social organisation. Rights are typically defined and refined in courts through legal concepts, often retroactively after an alleged breach of law. The concept of risk belongs to risk management practices within organisations, often defined through scientific concepts of probability in prospectively trying to deal with possible future consequences. This merger creates a novel object of assessment for which there is yet no method agreed upon.

6. The GDPR brought to the data protection fore terminology from risk management, such as 'high risk', 'likelihood', 'impact' or 'severity'. It is however very unclear what these terms mean in the context of personal data protection, or – more broadly – "*rights and freedoms of natural persons*". Several of these terms might not be directly relevant for, or difficult to square with, data protection law and could create artificial complications for the assessment process. In result, many of them will have to be given a new, autonomous meaning.

7. The GDPR links DPIAs with prior consultation should the assessment process indicate residual risks of a high level. It provides broad powers to DPAs, which can provide written advice and – should further measures be necessary – can even prohibit the envisaged data processing operations.

8. The GDPR provides criteria for when a DPIA should be performed. It offers however very little indication on the process itself and is largely silent on methodological issues. This minimalistic approach was meant to constitute a 'legal hook' to be complemented by specific methods for conducting a DPIA, nevertheless certain key elements remain unaddressed.

9. The GDPR requires a data controller during the DPIA process to consult data subjects or their representatives with due respect for legitimate secrecy. However, this requirement is comparatively weak as it is triggered only "*where appropriate*", concerns only data subjects (and not broader publics), and the GDPR does not give any indication when this should be the case. It also falls short on specifying who exactly should be consulted, how to identify them, when one can resort to representatives, what counts as legitimate representativity, as well as what means of contestability are available.

10. The GDPR remains silent as to the transparency of the DPIA process. In particular, there is no requirement to make a draft and the final report or a summary thereof publicly available.

11. There is a vague requirement for the European Data Protection Board (EDPB) to issue guidelines "*to encourage consistent application of* [the] *Regulation*" and issuing and keeping up-to-date methods for the DPIA might fall into the scope of this requirement. Only upon their issuance will it be possible to appraise these methods.

12. The GDPR leaves data controllers some amount of discretion in carrying out a DPIA, at least in two aspects: first, in determining whether the envisaged processing operations fall within the predefined high risk criteria; second, in whether residual risks are sufficiently high so as to trigger the DPA consultation obligation. Furthermore, by the very nature of the risk management process, data controllers choose, *inter alia*, the method of assessment and measures for risk mitigation. It is also for data controllers to choose qualified assessors and to ensure their independence, to

guarantee robustness of the whole process, and to appropriately document it. Data controllers are fully accountable for these methodological choices.

13. It is implied that the GDPR recognises geographical and cultural differences in the protection of personal data. In particular, national exemptions, concerning, e.g. the freedom of expression, are to be taken into consideration in the assessment process.

14. The GDPR is largely silent on the roles and responsibilities for the conduct of a DPIA. In particular, the role of a data protection officer (DPO) is unclear. The GDPR requires them only to advise the assessor on the assessment process, yet without any specification.

IV. Recommendations

The foregoing evaluation has proven that the DPIA requirement in the GDPR satisfies certain elements of best practice for impact assessments, yet it fails to do so on certain other aspects. Therefore, the authors will now offer recommendations for European policy-makers to 'close the gap' between these two. These recommendations will be three-fold: the authors first suggest broadening the scope of the DPIA requirement. They subsequently propose to develop multiple methods for the DPIA that would address omissions and shortcomings of Art 35 GDPR. Eventually, the authors suggest that both the EDPB and national DPAs should take the lead and become 'reference centres' on DPIA. The authors have also been realistic as to the probability of their recommendations being actually implemented, i.e. these recommendations rely on delegated 'rule-making' and advisory powers that the GDPR vests in both the EDPB, and national and regional DPAs.

A. Scope

1. The list of data processing operations falling under the DPIA requirement shall be expanded so that intrusive ones do not escape scrutiny. This list should be kept up-to-date.

2. Whenever intrusive initiatives fall outside the scope of the DPIA requirement in the GPDR, resorting to other types of assessments, e.g. privacy impact assessment (PIA), should be recommended.

B. Methods

3. The EDPB is best-positioned to issue and keep up-to-date EU-wide methods for conducting a DPIA. National and regional DPAs, in turn, are best-positioned to adjust them to local contexts, whilst respecting the harmonisation goals of the GDPR. Due to the relative novelty of the DPIA requirement, these methods should be carefully developed.

4. These methods should be adaptive:

a. There should exist multiple methods to conduct a DPIA, tailored to reflect the diversity of industry or governance sectors and the specific risks attached thereto. These methods need to respect legal, cultural, social or ethical differences in multiple jurisdictions;

b. They need to be reviewed periodically as the experience of conducting DPIAs grows and societal contexts change;

5. These methods should address in particular:

a. conditions for public participation (i.e. identification of stakeholders, including data subjects; provision of information; means for hearing their voices and taking them into consideration; and means for contestability);

b. conditions for documentation and transparency (i.e. written documentation, accessibility of DPIA-related information, public registers of performed DPIA, legitimate secrecy, etc.);

c. clarifications of vague terminology, especially quantitative (e.g. 'large scale') and risk-related terms (e.g. 'risk to a right', 'high risk' and 'likelihood');

d. clarifications as to the qualifications and independence of the assessor;

e. clarifications as to the roles, responsibilities and accountability of stakeholders involved in the DPIA process, in particular of data controllers, data processors and DPOs.

6. The methods should be receptive in their development and experiences from previous impact assessment attempts offer lessons to learn. More specifically, *legal* lessons on substance and procedure should to be taken into account to make the DPIA a discrete assessment tool. Procedural lessons pertain to public access to relevant information, public consultation and contestability. Substantive lessons pertain to the criteria for risk identification (to be learnt e.g. from data protection law), different types of risk (environmental law), new types of harm or impact (tort law) or degrees of probability (evidence law).

7. Conditions for oversight (audit) of the DPIA process by DPAs (and/or other stakeholders) should be defined, ranging from the criteria for process-based elements (e.g. the quality of the DPIA) to actor-based ones (e.g. the discretion asserted to data controllers).

C. Knowledge and know-how

8. Both the EDPB and national and regional DPAs should establish and maintain 'reference centres' with relevant knowledge and know-how on DPIA. These centres should cooperate with each other and become part of the larger impact assessment community by aligning with dedicated associations and/or conferences.

All in all, DPIAs are only an aid for decision-making. These impact assessments are no 'silver bullet' solutions: the quality of protection they can afford depends on the way data controllers and processors use them, on the support they would receive from policy-makers and – eventually – on the oversight from DPAs and courts of law. These impact assessments do not come without difficulties, yet with honest performance, and with policy-makers having methods in place, supplemented with guidance, advice and oversight, these assessments will ultimately contribute towards a more robust protection of personal data.

Selected relevant sources

Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review* 25, no. 2 (2009): 123–135, doi:10.1016/j.clsr.2009.02.002.

David Wright and Paul De Hert (eds.), *Privacy Impact Assessment* (Dordrecht: Springer, 2012), doi: 10.1007/978-94-007-2543-0.

Dariusz Kloza, Niels van Dijk, and Paul De Hert, "Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies," in *Smart Grid Security*, ed. Florian Skopik and Paul Smith (Waltham, MA: Elsevier, 2015), 11–47, doi:10.1016/B978-0-12-802122-4.00002-X.

Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, "A Risk to a Right? Beyond Data Protection Risk Assessments," *Computer Law & Security Review* 32, no. 2 (2016): 286–306, doi:10.1016/j.clsr.2015.12.017.

Raphaël Gellert, "We have always managed risks in data protection law: understanding the similarities and differences between the rights-based and the risk-based approaches to data protection," *European Data Protection Law Review* 2, no. 4 (2016): 481–492, doi:10.21552/EDPL/2016/4/7.

István Böröcz, "Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras," *European Data Protection Law Review* 2, no. 4 (2016): 467–480, doi:10.21552/EDPL/2016/4/6.

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 our 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 PIAF, ADVISE, EPINET, MATHISIS, FORENSOR, CANDID (co-funded by the EU), PARENT (co-funded by the EU and Innoviris) as well as "A Risk to A Right? Exploring a new notion in data protection law" and "Rights in Design. The Technological Reconstitution of Privacy and Data Protection" (funded by Fonds Wetenschappelijk Onderzoek – Vlaanderen). The views expressed in this policy brief do not reflect the views of any of these funding agencies.

We thank the following members of the d.pia.lab Network for their comments on an earlier version of this policy brief: Brendan van Alsenoy, Roger Clarke, Kjetil Rommetveit and Claudia Quelle. We thank Pradeepan Sarma for copy-editing.

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