Data protection impact assessment in the European Union: developing a template for a report from the assessment process

Kloza, Dariusz; Calvi, Alessandra; Casiraghi, Simone; Vazquez Maymir, Sergi; Ioannidis, Nikolaos; Tanas, Alessia; Van Dijk, Niels

Published in:
d.pia.lab Policy Brief

DOI:
10.31228/osf.io/7qrfp
10.5281/zenodo.4501295

Publication date:
2020

License:
CC BY-SA

Document Version:
Final published version

Data protection impact assessment in the European Union: developing a template for a report from the assessment process

d.pia.lab Policy Brief No. 1/2020

Dariusz KLOZA, Alessandra CALVI, Simone CASIRAGHI,
Sergi VAZQUEZ MAYMIR, Nikolaos IOANNIDIS, Alessia TANAS and Niels VAN DIJK

Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)
Research Group on Law, Science, Technology & Society (LSTS) | Vrije Universiteit Brussel (VUB)

This Policy Brief proposes a template for a report from a process of data protection impact assessment (DPIA) in the European Union (EU). Grounded in the previously elaborated framework (cf. Policy Brief No. 1/2017) and method for impact assessment (cf. Policy Brief No. 1/2019), the proposed template conforms to the requirements of Articles 35–36 of the General Data Protection Regulation (GDPR) and reflects best practices for impact assessment, offering at the same time five novel aspects. First, it aims at comprehensiveness to arrive at the most robust advice for decision making. Second, it aims at efficiency, that is, to produce effects with the least use of resources. Third, it aims at exploring and accommodating the perspectives of various stakeholders, although the perspective of individuals dominates; it, therefore, fosters fundamental rights thinking by, for example, requiring justification for each choice, hence going beyond a mere 'tick-box' exercise. Fourth, it aims at adhering to the legal design approach to guide the assessors in a practical, easy and intuitive manner throughout the 11-step assessment process, providing necessary explanations for each step, while being structured in expandable and modifiable tables and fields to fill in. Fifth, it assumes its lack of finality as it will need to be revised as experience with its use grows. The template is addressed predominantly to assessors entrusted by data controllers to perform the assessment process, yet it may also assist data protection authorities (DPA) in the EU to develop (tailored down) templates for DPIA for their own jurisdictions.

1 INTRODUCTION

1.1 CONTEXT

The European Union's (EU) General Data Protection Regulation (GDPR) imposes on data controllers, *inter alia*, an obligation to conduct, if there is a likelihood of a high risk to the rights and freedoms of natural persons, a process of data protection impact assessment (DPIA) (Article 35(1)). This novel requirement has already provoked a number of questions, and some of them concern the practical aspects of the assessment process. In response, the d.pia.lab in this Policy Brief proposes a *template* for a report from a process of DPIA that reflects best practices for impact assessment and, at the same time, conforms to the requirements of the GDPR.

A template for the assessment process is a practical aid to the assessors. It is a form to fill in that—following a given method—structures the assessment process, guides the assessors throughout it and, upon completion, serves as a final report therefrom. At the same time, it documents all the activities undertaken within a given assessment process, serving to demonstrate for controllers, *inter alia*, the extent of compliance with the law and providing evidence as to the quality of the assessment process (cf. the principle of accountability; Article 5(2)). A template for the assessment process can be seen as a practical implementation of a *method* (i.e., a procedure comprising consecutive and/or iterative steps) for impact assessment, itself reflecting a *framework* therefor (i.e., conditions and principles spelling out its theory and practice). Despite their benefits, templates for the process of impact assessment have their own inherent limitations and cannot be used without critical reflection.

1.2 STATE OF THE ART AND BEYOND

There is no consensus on *exactly* how to perform a process of impact assessment. Multiple templates for a process of DPIA have been developed that come in multiple shapes and with varying applicability (jurisdiction, industry or governance sector, etc.). The quality of these templates varies significantly. The most frequent problems seem to concern

 ISSN 2565-9936

their fitness-for-purpose, incomprehensiveness, little clarity and lack of detail, which eventually render them of little use to assessors.

The proposed template has been built on the critical and comparative analysis of the existing ones, refined with d.pia.lab's own experience. The template adheres to the principles and conditions set forth in the *framework* for impact assessment developed by d.pia.lab (cf. Policy Brief No. 1/2017, Sect. 2). It is built on the generic *method* for impact assessment (cf. Policy Brief No. 1/2019, Sect. 2), slightly revised and updated, and tailored down to the legal requirements in the EU (cf. Policy Brief No. 1/2019, Sect. 3). In other words, the template merges the generic method for impact assessment with the specific method for DPIA as interpreted from Articles 35–36, essentially by superimposing the latter onto the former. However, the template differentiates between compulsory and voluntary elements of the assessment process, and, as a result, any element not required *expressis verbis* by the GDPR is clearly marked as such.

The proposed template offers at least five novel aspects. First, it aims to be comprehensive, aiming to arrive at the most robust advice for decision making and, in so doing, aiming not to omit relevant societal concerns, stakeholders and steps to be undertaken in the assessment process, among others.

Second, the template aims for a DPIA process to be efficient, i.e., producing effects (such as advice for decision making) with the least use of resources, e.g., it allows for a choice of specific appraisal techniques or for the integration of multiple assessment processes. With a view to optimising the use of resources, it dedicates a specific step to plan and prepare a given assessment process.

Third, the template aims at exploring and accommodating the perspectives of various stakeholders (e.g., individuals, the public and private sectors), yet the perspective of individuals dominates. This is so because it is taken for granted that personal data—and related fundamental rights and freedoms—merit protection of a certain quality. Hence, the template aims at protecting individuals not only by helping controllers to comply with the law but also by going beyond mere formalism. By requiring elaborate justification for each choice made, it fosters data protection and fundamental rights thinking and steers the assessment process towards a more comprehensive activity rather than a mere compliance check, 'tick-box' exercise.

Fourth, the template aims to be user friendly. By adhering to the legal design approach—which aims to make legal systems and services more human-centred, usable and satisfying—this template not only guides the assessors step-by-step throughout the assessment process in a practical, easy and intuitive manner but also provides necessary yet minimal instructions and explanations.

Fifth and finally, the template assumes its lack of finality. Similar to frameworks and methods for impact assessment, as well as assessment processes themselves, a template is a 'living instrument' that continuously evolves as experience with its use grows and hence needs to be revised accordingly.

The proposed template is subjected to certain necessary limitations. First, being built upon a DPIA process as required by the GDPR, it *does not* consider the specificities of a DPIA process as required elsewhere in the EU, e.g., under Law Enforcement Directive 2016/680 or Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies (2018/1725). Second, the proposed template would rarely be directly applied. Instead, it will need to be tailored down to the context of use, such as a given jurisdiction, governance or industry sector.

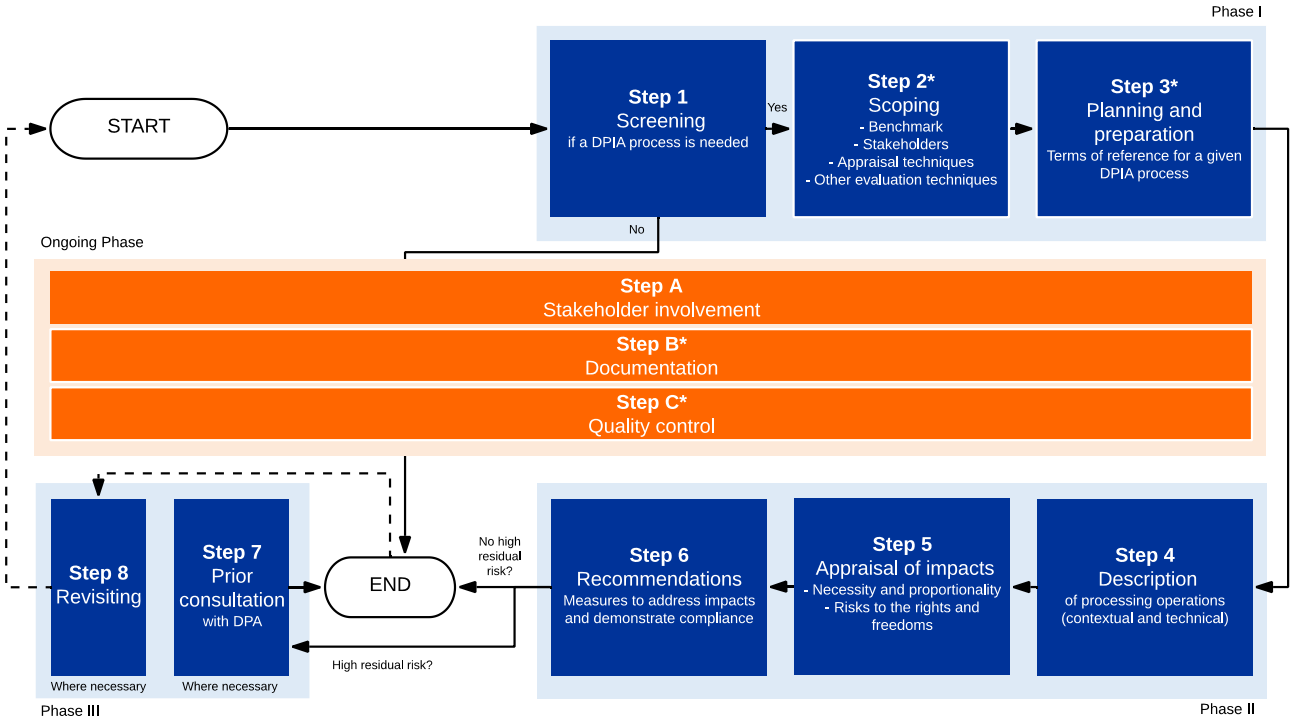
1.3 ADDRESSEES OF THE TEMPLATE

The proposed template is first and foremost meant to be used by assessors entrusted by the controller to perform a given DPIA process. Assessors are natural or legal persons that in practice perform the assessment process. The assessment process is rarely a single-person task; instead, a team of assessors with diverse knowledge and know-how would most often need to be assembled to accomplish such a collaborative process. Assessors can be in-house or outsourced against a fee (e.g., a consultancy), although the controller ultimately remains accountable (Article 5(2) and Article 24) and legally responsible for a given assessment process (Article 83(4)(a)). If controllers conduct the assessment process themselves, they become assessors.

In addition, the proposed template may influence the development of templates for a (tailored down) DPIA process that national and/or regional data protection authorities (DPAs) in the EU and other jurisdictions of the European Economic Area (EEA) might issue for their own jurisdictions. It may further serve as a blueprint for (bespoken) templates for a DPIA process in other jurisdictions and—potentially—for templates for other types of assessment processes in other domains of practice.

1.4 OVERVIEW OF THE ASSESSMENT METHOD

The proposed template reflects a method that consists of eleven steps, six of which are consecutive steps (Steps 1–6; Steps 1–3 might, to a large extent, be executed in parallel), two *ex post* steps (Steps 7–8, triggered only in certain conditions) and three ongoing steps (Steps A–C, to be performed throughout the entire assessment process in parallel to Steps 1–8), grouped in four phases (Phases I–III; the Ongoing Phase bears no numbering). The order of these steps is motivated by how each one informs the subsequent one.



1.5 How do assessors use the template?

In order to report from the assessment process, the assessors fill in, in an easily understandable language, the tables and/or other fields assigned to each step. To the extent possible, each answer is exhaustive and sufficiently motivated (described, explained, justified, etc.), equally for the criteria fulfilled and not fulfilled. Further rows can be added in each table, should there be a need or, should the space be insufficient, each element can be moved to an appendix. Alternatively, any of the tables and/or fields might be removed and the same information might be presented in some other format if the assessors deem it appropriate. Explanatory notes at the beginning of each step might be deleted upon the completion of the report. (In parallel to the present Policy Brief, the d.pia.lab offers an editable form to fill in.)

Following the 11-step method in this template, consecutive steps are marked in blue and the ongoing steps in orange. The assessors fill in only the fields coloured in light blue or light orange, respectively. A field for any further remarks or comments, if necessary, is provided at the end of each step. After the receipt of a filled-in report, the controller, in turn, fills in light green fields only.

The template assumes the team of assessors is familiar with the legal framework for personal data protection established by the GDPR. (References to legal provisions without any further specification pertain to the GDPR.) It also assumes minimum familiarity with the process of risk appraisal and with the criteria limiting the enjoyment of human rights, in particular those of necessity and proportionality. Nonetheless, the proposed template has to be read in conjunction with d.pia.lab's previous policy briefs in which the key concepts have been explained. Further references are suggested at the end of this policy brief.

The DPIA process is normally initiated by (the leadership of) the controller, with whom an obligation to conduct the DPIA process rests (Article 35(1)). The processor, if appointed, is obliged to assist a controller (Article 28(3)(f)); however, a processor might conduct the assessment process for their own remit on their own will. It is assumed that all the actors—from the controller and assessors to the data protection officer (DPO) to stakeholders—are involved in the entirety of the assessment process. As the assessment process concerns data processing operations that normally are not yet in place—instead, they will be carried out in the future—the assessors might rely on estimations and, at times, incomplete information.

Utmost efforts have been made to ensure the accuracy of the information provided. However, all of the information in this document is provided without any warranty. Neither the d.pia.lab nor individual authors assume any liability for any negative consequence suffered as a result of the use, misuse or reliance on this document.

A TEMPLATE FOR A REPORT FROM THE PROCESS OF DPIA

IDENTIFYING DETAILS

Name of the initiative and number, if applicable	
Name, contact information and other identifying details of:	
▪ data controller(s)	
▪ data processor(s), if applicable	
▪ person(s) in charge of the initiative (business owner)	
▪ assessor(s)	
▪ data protection officer(s) (DPO), if appointed	
▪ chief information security officer, if appointed	
▪ competent quality control body supervising the assessment process, if appointed	
▪ competent data protection authority(ies) (DPA)	
▪ anyone else involved, as practicable	
Version of the report	
Level of confidentiality of the report	☐ Public ☐ Confidential ☐ Specific *[Explain]*
Date and place of compilation of the report	
[Any other details, as practicable]	

EXECUTIVE SUMMARY

[Summarise the most significant information concerning the outcome of each step of the present DPIA process.]

PHASE I: PREPARATION OF THE ASSESSMENT PROCESS

STEP 1 SCREENING (THRESHOLD ANALYSIS)

Objective

The goal of this step is to determine if the DPIA process is ever required because one or more of the criteria set forth by law or other relevant regulatory requirements are met or, alternatively, to determine if the assessment process is not required because an exemption is provided thereby.

EXTRA Nonetheless, the controller might decide to perform the DPIA process on their own will, regardless of the legal requirements, also as a means to assist in their compliance with the principle of accountability (Article 5(2), Article 24), data protection by design and by default (Article 25) and security of processing (Article 32).

Implementation

In this step, on the basis of some rudimentary contextual and technical descriptions of the envisaged data processing operations that constitute the initiative under assessment (cf. *Step 1a*), the assessors analyse whether the said operations satisfy any of the threshold criteria (cf. *Step 1b*). As a prerequisite, the assessors determine if personal data would be processed; if not, the GDPR does not apply and the DPIA process is hence not compulsory.

The criteria are set predominantly by the GDPR and might be supplemented by any other legal or otherwise regulatory instrument to which the controller is subject, e.g., a code of conduct (Article 40) (cf. *Step 2a*); case law might provide further clarification of these criteria.

Although not much information is usually available at the early stages, the preliminary description is kept short (ca. one page) yet is sufficiently detailed to the extent that the assessors can determine if the threshold criteria are satisfied. Such a description can be based on the records of processing operations, if available (Article 30). General statements are avoided. If it is determined that the assessment process is required, this preliminary description will be expanded in *Step 4*.

The threshold criteria are based on the concept of risk (explained in *Step 5*) and are either positive or negative. (Negative criteria take precedence over the positive ones.) If any of the positive criteria are satisfied, the assessment process will then be required by law. By contrast, if any of the negative criteria are satisfied, the controller is exempted from conducting the assessment process. In the former situation, the assessors proceed to *Step 2*.

EXTRA In the latter situation, the assessors prepare a statement of no significant impact, justifying the reasons for not performing a DPIA process and do not proceed further unless there is a need to revisit the assessment process (cf. *Step 8*). In case of doubt, it is recommended to conduct the assessment process.

STEP 1A: PRELIMINARY DESCRIPTION OF THE ENVISAGED PROCESSING OPERATION(S)

			Explanation
	Will you ever process personal data?		☐ Yes ☐ No
Contextual description	**Nature** *(what types of processing operations?)*		
	Scope	Scale (*how much? how many? how far?*)	
		Time *(when? how long?)*	
	Context (*in what circumstances*?)	Internal (*concerning the controller*)	
		External (*concerning individuals, groups, the society, etc.*)	
	Purpose of processing operations *(why?)*		
Technical description	Categories of personal data processed *(what?)*		
	Means of processing (infrastructure) *(by what means? e.g., analogue, digital)*		
	Envisioned data flows (*from where to where? from whom to whom?*)		
	Data security *(how is it ensured?)*		
	Jurisdiction/market (*where?*)		
	Actors in the 'supply chain' (*who?*)		
	[Other, specify]		

STEP 1B: SCREENING (THRESHOLD ANALYSIS)

Positive criteria

Criterion	*Legal provision*	*Satisfied?*	*Explanation*
CRITERION 1: LIKELIHOOD OF HIGH RISK (GENERAL) *Are the envisaged processing operations likely to result in a high risk to the rights and freedoms of natural persons?* to be determined on the basis of: ▪ risk indicators (nature, scope, context and purposes of processing) ▪ rudimentary risk assessment *(how likely? how severe?)* ▪ existing data protection risks registry (if any) ▪ *[other; specify]*	35(1)	☐	
CRITERION 2: LIKELIHOOD OF HIGH RISK (SPECIFIC) *Do the envisaged processing operations involve any of the situations deemed by law as likely to result in a high risk?* namely:			
▪ systematic and extensive evaluation of personal aspects relating to natural persons 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	35(3)(a)	☐	
▪ processing, on a large scale, of special categories of data, or personal data relating to criminal convictions and offences	35(3)(b)	☐	
▪ systematic monitoring of a publicly accessible area on a large scale	35(3)(c)	☐	
CRITERION 3: LIKELIHOOD OF HIGH RISK (POSITIVE ENUMERATION) *Are the envisaged processing operations included in the public list of processing operations, compiled by DPA(s), that require a DPIA process?*	35(4)	☐	
CRITERION 3 BIS: APPROVED CODES OF CONDUCT *Does an approved code of conduct require a DPIA process for the envisaged processing operations?*	40	☐	
[Other, cf. Step 2a*; specify]*		☐	
Is a DPIA process required?		☐	**Yes** *[go to Step 2]*
		☐	**No** *[go to Step 1c]*

Negative criteria

Criterion	*Legal provision*	*Satisfied?*	*Explanation*
CRITERION 4: LIKELIHOOD OF HIGH RISK (NEGATIVE ENUMERATION) *Are the envisaged processing operations included in the public list of processing operations, compiled by DPAs, exempted from a DPIA process?*	35(5)	☐	
CRITERION 5: PREVIOUS (REGULATORY) IMPACT ASSESSMENT *Have the envisaged processing operations already been subjected to an earlier assessment process?*	35(10)	☐	
CRITERION 6: EXEMPTIONS FOR SPECIFIC PROFESSIONS *Do the envisaged processing operations concern personal data from clients or patients by physicians, healthcare professionals or lawyers, therefore not considered on a large scale?*	Recital 91	☐	
CRITERION 6 BIS: APPROVED CODES OF CONDUCT *Does an approved code of conduct exempt the envisaged processing operations from a DPIA process*?	40	☐	
[Other, cf. Step 2a*; specify]*		☐	
Is the data controller exempted from a DPIA process?		☐	**Exempted** *[go to Step 1c]*
		☐	**Not exempted** *[go to Step 2]*
If exempted, is a DPIA process to be carried out voluntarily?		☐	**Yes** *[go to Step 2]*
		☐	**No** *[go to Step 1c]*

STEP 1C: STATEMENT OF NO SIGNIFICANT IMPACT EXTRA

[If criteria from 1 to and including 3bis are NOT met, why are the envisaged processing operations exempted from a DPIA process?]

COMMENTS

[Explanation]

STEP 2* SCOPING

Objective

The goal of this step is to identify, with some reasonable precision:

a) the benchmark, that is, a given standard of the fundamental right to personal data protection and of related fundamental rights and freedoms reflected in the applicable legal framework;

b) the categories of stakeholders, that is, those to involve in the assessment process and how to involve them in each step (i.e., stakeholder involvement techniques);

c) appraisal techniques, other than the necessity and proportionality assessment, and risk assessment, to be used in the assessment process, if any; and

d) other evaluation techniques that might be warranted or necessary.

Implementation

BENCHMARK. In the DPIA process, the benchmark consists of a given standard of: (a) the fundamental right to personal data protection and (b) other fundamental rights and freedoms affected by the envisaged processing operations (cf. Article 1(2); Recital 4). In this step, the assessors first map the aspects thereof that the envisaged data processing operations would touch upon. (Not all processing operations would trigger all provisions of the GDPR and of other relevant laws.) As these rights are regulated by multiple laws and other regulatory instruments, this is accompanied by a mapping of the legal framework applicable in a given jurisdiction.

STAKEHOLDERS. In this step, the assessors subsequently identify the categories of stakeholders to be consulted, namely—first and foremost—data subjects (e.g., employees, clients, customers, patients, students, pupils or pensioners) and/or their representatives (e.g., non-governmental organisations, associations or advocacy groups). However, such consultation also includes other individuals affected, affecting, concerned by or merely interested in the envisaged processing operations and/or their representatives as well as experts. Stakeholders are understood most broadly, and their range and number to be involved is commensurate to the processing operations. Stakeholders might suggest further stakeholders. (The specific individuals, groups and/or organisations to consult are determined in *Step 3*.) Stakeholders are *not* assessors; the former provide input, which subsequently the latter take into account or reject.

In the spectrum of stakeholder involvement (typically ranging from mere communication to co-decision), the GDPR sets it in the middle, at consultation, i.e., their views are sought and taken into consideration. Nonetheless, the controller might choose, on their own will, a higher level of stakeholder involvement in a given DPIA process.

Possible techniques to involve stakeholders range from a wide variety of events (workshops, focus groups, citizen juries) to polling (interviews, surveys, structured or semi-structured questionnaires) to written statements.

APPRAISAL TECHNIQUES. In the DPIA process, the GDPR foresees the use of two types of appraisal techniques: (a) necessity and proportionality assessment (Article 35(7)(b)), and (b) risk assessment (Article 35(7)(c)). Should these two prove to render insufficient information for decision making, other appraisal techniques might be employed, e.g., scenario analysis (planning), technology foresight or cost–benefit analysis (CBA). The GDPR does not specify exactly what appraisal technique is to be used, leaving the choice for the controller. Appraisal techniques are scientifically sound, legally valid (i.e., conform to the letter of the law) and replicable (i.e., an auditor or a judge could verify the results with the use of the same method).

OTHER EVALUATION TECHNIQUES. The assessors might resort to some other evaluation techniques, beyond DPIA, which may be warranted or required by law in order to, e.g., ensure the completeness of the information used in the decision-making process. For example, if the envisaged processing operations *also* affect the natural and/or human environment, together with a DPIA process, a standalone process of environmental impact assessment (EIA) may be warranted or required by law. A CBA may be employed as a standalone evaluation technique to determine if the benefits of the envisaged processing operations outweigh their costs.

In addition, for the reasons of comprehensiveness and efficiency, various types of impact assessment and other evaluation techniques can be integrated, provided the benchmark and/or appraisal techniques are coherent, not subordinated to each other and are not internally contradictory. Results of such an integrated assessment process must then be synthesised.

STEP 2A: BENCHMARK

Benchmark (1): Applicable laws and regulations

	Applicable laws and regulations	*Legal provision*	*Applicable?*	*Explanation*
lex generalis	General Data Protection Regulation (GDPR)		☒	
	National law(s) supplementing the GDPR		☒	
	Law Enforcement Directive 2016/680 [national transposition]		☐	
	[Other, specify]		☐	
lex specialis	ePrivacy Directive [national transposition]		☐	
	National exclusion/inclusion list(s)	35(4)–(5)	☐	
	Approved codes of conduct	40	☐	
	Certificates	42	☐	
	Adequacy decision(s)	45	☐	
	Binding corporate rules (BCR)	47	☐	
	Standard contractual clauses (SCC)	46(2)(c)–(d) 46(3)(a)	☐	
	[Other, specify]		☐	

other	Regulation 2018/1725		☐	
	Technical standards		☐	
	Data protection policies		☐	
	Professional codes of conduct *(e.g,. ethics, corporate governance, etc.)*		☐	
	Data sharing agreement(s)		☐	
	[Other, specify]		☐	

Benchmark (2): Scope of the assessment process

	Scope of the assessment process		*Legal provision*	*Applicable?*	*Explanation*
right to personal data protection	Personal data protection principles		5	☒	
	Legal basis for processing		6–8	☒	
	Processing of special categories of personal data		9–10	☐	
	Data subject rights	Transparency and information	12–14	☒	
		Right of access	15	☒	
		Right of rectification	16	☒	
		Right to erasure	17	☐	
		Right to restriction of processing	18	☒	
		Right to data portability	20	☐	
		Right to object	21	☐	
		Right to not be subject to automated decision making	22	☐	
	Obligations of data controller and of processor		24–39	☒	
	Data transfers outside EU/EEA		46–49	☐	
	Restrictions of obligations and rights		23	☐	
	Specific processing situations		85–91	☐	
	[Other, specify]			☐	

other fundamental rights	Private and family life, home and communications	Recital 4	☐	
	Freedom of thought, conscience and religion		☐	
	Freedom of expression and information		☐	
	Freedom to conduct a business		☐	
	Right to an effective remedy and to a fair trial		☐	
	Cultural, religious and linguistic diversity		☐	
	[Other fundamental rights, specify]	CFR	☐	
[Other aspects of personal data protection, specify]			☐	

STEP 2B: STAKEHOLDERS, THE LEVEL OF THEIR INVOLVEMENT AND THEIR INVOLVEMENT TECHNIQUES

Internal stakeholders

Category of stakeholder	*Involved?*	*Level of involvement*	*Stakeholder involvement technique(s)*	*Explanation*
Data processor(s)	☐			
Data protection officer(s) (DPO)	☐			
Recipient(s) (Article 4(9))	☐			
Representative(s) (Article 27)	☐			
Information security officer(s)	☐			
Legal service	☐			
Employees, trade unions, contractors, etc.	☐			
[Other, specify]	☐			

External stakeholders

Category of stakeholder		*Involved?*	*Level of involvement*	*Stakeholder involvement technique(s)*	*Explanation*
Data subjects(s), including: ▪ minors ▪ vulnerable people ▪ *[other, specify]*		☐			
Representative(s) of data subject(s)		☐			
Individuals who are not data subjects		☐			
Representative(s) of individuals who are not data subjects		☐			
Third parties (Article 4(10))	public sector	☐			
	private sector	☐			
Experts		☐			
Supervisory authority(ies) (DPA)		☐			
[Anybody else affected, etc., specify]		☐			

Lack of stakeholder involvement

[If stakeholders are not to be involved in the present DPIA process, explain why.]

STEP 2C: APPRAISAL TECHNIQUES

	Type of appraisal techniques	*Legal provision*	*Applicable?*	*Specific technique(s)*	*Explanation*
Mandatory	Necessity and proportionality assessment	35(7)(b)	☒		
	Risk assessment (rights and freedoms of natural persons)	35(7)(c)	☒		
	[Other, cf. Step 2a*; specify]*		☐		
Supplementary	Risk assessment (data security)		☐		
	Scenario planning		☐		
	Cost–Benefit Analysis (CBA)		☐		
	Strengths, Weaknesses, Opportunities, Threats (SWOT)		☐		
	[Other, specify]		☐		

STEP 2D: OTHER EVALUATION TECHNIQUES

Types of evaluation techniques	*Applicable?*	*Specific technique(s)*	*Explanation*
Environmental impact assessment (EIA)	☐		
Privacy impact assessment (PIA)	☐		
Ethics impact assessment	☐		
Social impact assessment	☐		
Health impact assessment	☐		
Risk assessment	☐		
Cost–Benefit Analysis (CBA)	☐		
Strengths, Weaknesses, Opportunities, Threats (SWOT)	☐		
[Other, specify]	☐		

INTEGRATED IMPACT ASSESSMENT

	Explanation
Elements of the benchmark	
Appraisal technique(s)	
[Other, specify]	

COMMENTS

[Explanation]

STEP 3* PLANNING AND PREPARATION

Objective

The goal of this step is to set the terms of reference for a given DPIA process. This step answers the question of how to conduct a given DPIA process, constituting a written manual therefor, and it might be updated throughout the assessment process. Not all its elements, however, are of equal importance and applicability.

Implementation

SPECIFIC OBJECTIVES OF A GIVEN DPIA PROCESS. At a general level, at a minimum, the *substantive* goal of a DPIA process is to ensure the highest possible level of protection of individuals whose personal data would be processed in the envisaged operations. The *formal* goal thereof is to comply with the law (cf. Article 35(7)(d)). A DPIA process aims at ensuring both goals by aiding the decision-making process as to the deployment of the envisaged processing operations and their shape. However, the controller clarifies in greater detail the specific objectives of a given assessment process.

ACCEPTABILITY CRITERIA OF NEGATIVE IMPACTS. The controller sets and justifies the criteria for the acceptability of negative impacts. Such a threshold is set and justified for each appraisal technique employed (cf. *Step 2c*). The controller sets and justifies a threshold below which a processing operation would be deemed unnecessary and/or disproportionate, given the legal or cultural context.

The controller also sets a threshold above which a risk to a right would not be accepted, given the legal or cultural context or the risk attitude (e.g., risk-prone or risk-adverse). In other words, the controller specifies the level of risk that is acceptable. The controller defines beforehand both the likelihood and severity scales.

RESOURCES TO BE COMMITTED. The controller lists and ensures necessary resources to conduct a DPIA process, which include, but are not limited to: time (hours, days or months to be devoted to accomplish an entire DPIA process); money (cost of labour, equipment, stakeholder involvement, etc.); workforce (number of persons, part-time or full-time, to be involved in a DPIA process); knowledge (assessors' expertise, e.g., legal, ethical, data literacy, computer science, project management, public relations, etc.); know-how (experience required by the persons involved in a DPIA process); premises (place(s) where a DPIA process will be performed) and infrastructure (assets required for a DPIA process, e.g., hardware and software). Assessors might resort to the help of software that facilitates the DPIA process by automating parts thereof.

PROCEDURES AND TIMEFRAMES. The controller sets up the timeframes for a DPIA process, specifying, e.g., milestones and deadlines, assigning responsibilities for the assessors and specifying who is answerable to whom within the organisational structure of the controller.

(TEAM OF) ASSESSORS, AND THEIR ROLES AND RESPONSIBILITIES. The assessment process requires multiple types of expertise. The controller, on the basis of transparent criteria, chooses the assessors, either internal or external (outsourced) or a combination thereof. The (team of) assessors might be changed and/or expanded as the assessment process progresses. If the assessment process is outsourced, entirely or in part, the controller concludes a service contract with external assessors. The controller spells out their roles and responsibilities (e.g., to whom the assessors report), and ensures their professional independence (e.g., assessors do not seek nor receive instructions; their bias is explicitly marked as such).

STAKEHOLDERS. Based on the pre-defined categories in *Step 2b*, the assessors identify stakeholders, having regard to ensuring their diversity (e.g., gender balance, geographic diversity, age diversity or multidisciplinarity) and—if any direct stakeholder involvement techniques are to be used—also their contact details. Depending on its length, this list can be either filled-in on this template or appended thereto. For large-scale consultations, a consultation plan might be necessary. Personal data of identified stakeholders is appropriately protected.

CONTINUITY. The controller specifies the continuity of the assessment process in case of, e.g., changes in the actors involved in the assessment process (e.g., controller, processors, assessors, etc.), disruption, natural disasters or utility failures.

REVISION. The controller specifies the criteria triggering the revision of the DPIA process. The GDPR foresees, at a minimum, a change in the level of risk (cf. Article 35(11)) (cf. *Step 8*).

STEP3A: OBJECTIVES OF THE ASSESSMENT PROCESS

Objective	*Applicable?*	*Explanation*
Protection of individuals	☒	
Compliance with the law	☒	
[Other, specify]	☐	

STEP 3B: CRITERIA FOR THE ACCEPTABILITY OF NEGATIVE IMPACTS

Evaluation technique		*Explanation*
Necessity and proportionality (Article 35(7)(b))		
EXTRA Human rights limitation criteria (Article 52(1) CFR)		
Risk assessment (qualitative, quantitative) *(risk criteria)*	Likelihood scale	
	Severity scale	
	Point of acceptability	
[Other, specify]		

STEP 3C: RESOURCES TO BE COMMITTED

	Value	*Explanation*
Time (*how long?)*		
Money (*how much?*)		
Workforce (*how many people?*)		
Knowledge (*what expertise?)*		
Know-how (*what experience?*)		
Premises (*where?*)		
Infrastructure (*by what means?*)		
[Other, specify]		

STEP 3D: PROCEDURES AND TIME-FRAMES FOR THE ASSESSMENT PROCESS

	Milestone	*Deadline*	*Responsibility*	*Supervision*
1	*[Specify]*			
2				

STEP 3E: ASSESSORS, ROLES AND RESPONSIBILITIES

	Name	*If external: organisation*	*Contact details*	*Expertise*	*Roles and responsibilities*	*Other information*
1	*[Specify]*				*[Leader]*	
2						

STEP 3F: STAKEHOLDERS

[Provide contact details of all stakeholders to involve in the present DPIA process and a consultation plan, if necessary.]

STEP 3G: CONTINUITY OF THE ASSESSMENT PROCESS

[How would the present assessment process be continued in case of a disruption, reorganisation, etc. of the controller?]

STEP 3H: CRITERIA TRIGGERING THE REVISION OF A DPIA PROCESS

Criterion	*Applicable?*	*Explanation*
Change of likelihood and/or severity of a risk	☒	
[Other, specify]	☐	

COMMENTS

[Explanation]

ONGOING STEPS FOR PHASE I

STEP A STAKEHOLDER INVOLVEMENT

Objective

The goal of this ongoing step is to consult (seek the views), throughout the entire process, of data subjects and/or of their representatives, if practicable, on the envisaged processing operations (Article 35(9)).

EXTRA In addition, the assessors might decide to involve further stakeholders and at a broader level.

Implementation

Stakeholders are typically identified, informed, involved (consulted) and, eventually, they have their views considered.

Stakeholders whose categories have been stipulated in *Step 2b* are further identified in *Step 3f*. Their involvement is continuous and they are asked about their views on the subject matter of each step. (Their involvement is grouped *per* phase of the assessment process.)

Information given and sought is robust, accurate, inclusive and meaningful. Information is given to stakeholders in a plain language and hence it might require preparation of specific documentation, e.g., technical briefings. Stakeholders are involved with due respect for confidentiality, i.e., state secrets, trade secrets, personal data or otherwise privileged information.

Having gathered the viewpoints of the stakeholders, the assessors consider and take position on their views, i.e., whether they accept them or not; especially if the latter, the assessors provide exhaustive justification therefor.

Both stakeholder involvement and quality control (cf. *Step B*) are reported after the conclusion of each phase of the assessment process. After the first phase, the assessors and the quality control bodies are interested in whether a decision to perform a DPIA process was correct and, if so, whether the scope of the assessment process and its terms of reference were correct. After the second phase, they are interested in whether the impacts have been correctly appraised. After the third phase, if triggered, they are interested in whether the residual risks have been correctly appraised and/or whether the assessment process needs to be performed again.

	Stakeholder(s) identified	*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g,. opinion)?*	*How was their input included? Why was it rejected?*
internal	Data processor(s)			
	Data protection officer(s) (DPO)			
	Recipient(s) (Article 4(9))			
	Representative(s) (Article 27)			
	Information security officer(s)			
	Legal service			

	Employees, trade unions, contractors, etc.			
	[Other, specify]			
external	Data subjects(s)			
	Representative(s) of data subject(s)			
	Individuals who are not data subjects			
	Representative(s) of individuals who are not data subjects			
	Third parties (Article 4(10)) — public sector			
	Third parties (Article 4(10)) — private sector			
	Experts			
	Supervisory authority(ies) (DPA)			
	[Other, specify]			

Lack of stakeholder involvement in the present phase

[If stakeholders are not involved in the present phase of the DPIA process, explain why.]

STEP B* QUALITY CONTROL

Objective

The goal of this ongoing step is to check, internally and/or externally, throughout the entire assessment process, whether a DPIA process adheres to a given standard of performance and to remedy, if necessary, any irregularities.

Implementation

Quality control can be internal, external or both, and take the form of monitoring, review, audit, etc. The controller might require the team of assessors to be updated regularly or *ad hoc* on the progress of the assessment process, might establish a progress monitoring tool or an internal advisory board. (Professional independence of the assessors remains guaranteed.) In parallel, the DPO is tasked to monitor and advice on a DPIA process. The external quality control may be performed by an audit organisation hired by the controller or, alternatively, by a DPA, either upon request of the controller or on its own motion (e.g., when required by law).

The quality control can be structured, permanent (recurring in all the steps of the process) or performed on an *ad hoc* basis; it can be formal (e.g., concerning the compliance with the procedures for a DPIA process) or substantive (e.g., if the risks were appropriately assessed); and can occur during the process or afterwards. In case of judicial claims, courts of law will review a DPIA process, either as to its form, its substance or both.

Quality control body	*What feedback was received?*	*How was the feedback implemented? Why was it rejected?*
Data protection officer(s) (DPO)		
Supervisory authority (DPA)		
[Other, specify]		

Lack of quality control in the present phase

[If the quality was not controlled in the present phase of the DPIA process, explain why.]

COMMENTS

[Explanation]

PHASE II: ASSESSMENT

STEP 4 SYSTEMATIC DESCRIPTION

Objectives

The goal of this step is, by expanding the preliminary description (cf. *Step 1a*), to systematically describe the envisaged processing operations both contextually and technically.

Implementation

The systematic description concerns both contextual and technical aspects of the envisaged processing operations as well as any other useful information. Contextual aspects concern the nature (inherent characteristics), scope (size and range, e.g., duration, budget, complexity, etc.), internal and external context (circumstances) and purposes (aims) of the envisaged processing operations and, when applicable, the legitimate interest pursued by the controller. A diagram of data flows and/or other visualisations might be appended. Such a description can be based on the records of processing operations (Article 30). General statements are avoided. The said description might undergo changes as the assessment process progresses.

The systematic description expands the preliminary one (cf. *Step 1a*) and hence is much lengthier. It is sufficiently complete, accurate and reliable as it constitutes a basis for the analysis of impacts in *Step 5*.

A SUCCINCT DESCRIPTION OF THE ENVISAGED INITIATIVE

[Explanation]

A DETAILED DESCRIPTION OF THE ENVISAGED INITIATIVE

				Explanation
Contextual description	**Nature** *(what types of processing operations? E.g., collection, storage, erasure, etc.)*		1	
			2	
			…	
	Scope	Scale (*how much? how many? how far?*)		
		Time *(when? how long?)*		
	Context (*in what circumstances*?)	Internal (*concerning the controller*)		
		External (*concerning individuals, groups, the society, etc.*)		
	Purpose of processing operations, including, where applicable, legitimate interest *(why?)*			
	EXTRA **Benefits** of processing operations	for individuals, including data subjects		
		for the data controller		
		for the society as a whole		
	EXTRA **Drawbacks** of processing operations	for individuals, including data subjects		
		for the data controller		
		for the society as a whole		
Technical description	Categories of personal data *(what?)* ▪ *special categories of personal data* ▪ *personal data of vulnerable people (e.g., children)* ▪ *data of a highly personal nature*			

Means of processing (infrastructure) *(by what means?)*	
Envisioned data flows (*where to where? whom to whom?*)	
Data security *(how is it ensured?)*	
Jurisdiction/market (*where?*)	
Actors in the 'supply chain' (*who?*)	
[Other, specify]	

DIAGRAM OF (PERSONAL) DATA FLOWS AND/OR OTHER VISUALISATIONS

[Insert a diagram]

COMMENTS

[Explanation]

STEP 5 APPRAISAL OF IMPACTS

Objectives

The goal of this step is to assess the necessity and proportionally of the envisaged processing operations in relation to their purposes, and to assess the risks to the rights and freedoms of individuals stemming therefrom.

Implementation

The assessors use specific appraisal techniques pre-defined in *Step 2c* and base their analysis on the results of *Step 4*. The assessors can use any of the few suitable methods available thus far or they can use the one proposed in the present template. Contrary to methods for assessing risk (e.g., international standards, such as ISO 31000:2018 or ISO 27005:2018), methods for assessing proportionality and necessity in the context of personal data protection are rather scarce.

NECESSITY AND PROPORTIONALITY ASSESSMENT. The assessment of necessity and proportionality might occur at two levels. First, each data processing operation is assessed against personal data protection principles (cf. level 1). These are: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (Article 5(1), including security of processing (Article 32)) and data protection by design and by default (Article 25). Each data processing operation is assessed in a specific table and such a table needs to be replicated for each data processing operation.

EXTRA Second, given the fact that a fundamental right is at stake and that an assessment process of the envisaged processing operations against solely personal data protection principles (level 1) might not always be sufficiently complete to the detriment of the level of protection and the quality of the decision-making process it is meant to advise, the assessors might expand their appraisal to the entirety of human rights limitation criteria. In other words, while it is assumed that the entirety of the provisions of the GDPR, and especially the personal data protection principles, is meant to observe the human rights limitation criteria (Article 52(1) Charter of Fundamental Rights of the EU (CFR)) (level 1), there might still exist instances that would question such assumption and, therefore, in which the envisaged initiative under assessment must be examined against the entirety of these limitation criteria (level 2). For example, despite a presumption of conformity with fundamental rights, a provision of the GDPR might be, entirely or in part, in conflict therewith; furthermore, so might be a national exemption or derogation from the GDPR (e.g., processing carried out for journalistic purposes or the purposes of academic, artistic or literary expression; Article 85). However, such broader appraisal might be applicable only to specific controllers and/or to specific data processing operations (e.g., a task carried out for a public interest).

As the right to personal data protection and (the majority of) related fundamental rights are not absolute but rather relative ones (i.e., an interference with the right can only be justified under certain conditions), these five limitation criteria following Article 52 CFR can be read as follows:

- *legality* (i.e., if a basis for a data processing operation is 'provided for by law' of a sufficient quality, e.g., clarity, accessibility, precision, foreseeability, conformity with the rule of law);
- the respect for the *essence* of a right (i.e., if the interference with a fundamental right does not make it impossible to exercise a right);
- *legitimacy* (i.e., if a processing operation serves a given 'general interest' (cf. e.g., Article 3 Treaty on European Union (TEU)) or 'protect[s] the rights and freedoms of others');
- *necessity* (i.e., if a processing operation is 'necessary and [if it] genuinely meet[s]' legitimate objectives); and
- *proportionality sensu stricto* (e.g., balancing) (e.g., if the least intrusive option has been chosen).

Furthermore, it is argued under the doctrine that the *suitability* of a processing operation should also be assessed, i.e. whether a processing operation is suited (ever capable) to achieve a given legitimate aim.

By virtue of Article 52(3) CFR, the 'meaning and scope' of the rights, including their limitation criteria, 'shall be the same as those laid down' in the European Convention on Human Rights (ECHR).

RISK ASSESSMENT. On the grounds of the GDPR, risk is understood as a negative consequence arising from processing operations that might or might not occur in the future. Such a consequence, if it materialised, would produce physical, material or non-material damage to natural persons (largely, data subjects) and *not* solely to the controllers or

processors. Risk assessment is meant to be as objective as possible (Recitals 75–76); this is, however, not always attainable in practice, due to ambiguities about assignable likelihoods and possible types of damage, and by taking into account 'subjective' perceptions of risk by stakeholders (e.g., data subjects).

Risk is typically assessed by combining two measurements, namely its likelihood or probability (i.e., chance of happening) and its severity (i.e., magnitude of consequences) (Recital 76). Risk can be assessed qualitatively, quantitatively or with a combination of both. There are aspects of personal data protection that fit into the former (i.e., risk to rights and freedoms) and to the latter (e.g., data security). Quantitative risk assessment measures the probability of occurrence of a risk and combines it with its severity. Probability is expressed on a scale ranging from 0 to 1. In turn, qualitative risk assessment instead uses levels of likelihood (e.g., a 4-partite descriptive scale of negligible, low, medium and high) to be combined with its severity. Eventually, severity of a risk indicates a magnitude of damage should a risk materialise. It can be equally expressed on a 4-partite descriptive scale. Both scales—likelihood and severity—are pre-defined and justified in *Step 3b*.

A typical method for risk assessment requires, first, the identification of a risk, i.e., to find, recognise and describe it. (Knowledge bases might be of use here.) In the second step, the risk is analysed, i.e., its nature is comprehended in order to determine the level of risk, e.g., by multiplying the likelihood (probability) of its occurrence by the severity of its consequences. In the third step, the risk is evaluated, i.e., the results of risk analysis are compared with the risk criteria (cf. *Step 3b*) in order to determine whether the risk and its level are acceptable, if any mitigation measure is to be recommended and if any risk should be prioritised. (Risk treatment lies outside the risk assessment process and, hence, constitutes part of a separate process.)

STEP 6 RECOMMENDATIONS

Objective

The goal of this step is to suggest measures to address the risks and unnecessity and disproportionality of the processing operations identified in the previous step in order to protect individuals and to demonstrate compliance with law, 'taking into account the rights and legitimate interests of data subjects and other persons concerned' (Article 35(7)(d)).

EXTRA Assessors might suggest measures to maximise positive impacts.

Implementation

The assessors recommend and describe mitigation measures for each negative impact (risks, disproportionate and unnecessary interferences) identified in *Step 5*. Recommendations suggested are those of means (best efforts obligations) and not those of results.

For each personal data protection principle (level 1) and/or human rights limitation criterion (level 2) *not* satisfied in the previous step, the assessors recommend measures to satisfy these principles and/or criteria.

Each risk is mitigated by manipulating either its likelihood (probability)—by, e.g., limiting the exposure to a risk—or its severity—by, e.g., preparing a response plan should the risk materialise—or both. Risks can be avoided, mitigated, transferred (to another entity, e.g., outsource, insurance, etc., or in time) or accepted. Residual risk is a risk that remains if there is no measure available to mitigate it and triggers a prior consultation with a DPA (cf. *Step 7*).

For both risk and unnecessity and disproportionality, mitigation measures can be of a regulatory (legal), technical, organisational or behavioural nature. (Knowledge bases might be of use here.) The assessors might first take stock of measures already planned or already in place. The assessors conclude this step with an implementation plan in which the person responsible for the implementation of each measure and its deadline are provided.

Upon the receipt of the report, the leadership of the controller makes a decision as to the deployment of an envisaged initiative and—if it decides to go forward—under what conditions. More concretely, having received the report, the leadership of the controller takes a position on each of the recommendations proposed by the assessors. If they reject or change any of them, they provide exhaustive justification therefor. Upon the agreement with the controller, some recommendations might already be implemented during the assessment process.

NECESSITY AND PROPORTIONALITY OF THE PROCESSING OPERATIONS

Level 1: Personal data protection principles

ID of a processing operation	
Type of a processing operation	

STEP 5 APPRAISAL OF IMPACTS | **STEP 6 RECOMMENDATIONS**

Principle		*Legal provision*	*Applicable?*	*Satisfied?*	*Explanation*	*Response plan, if principle not satisfied*				
						Measures in place	*Measures to introduce*	*Responsible person*	*Priority*	*Deadline*
Lawfulness	Consent	6(1)(a)	☐	☐						
	Contract	6(1)(b)	☐	☐						
	Legal compliance	6(1)(c)	☐	☐						
	Vital interests	6(1)(d)	☐	☐						

	Public interest	6(1)(e)	☐	☐						
	Legitimate interests	6(1)(f)	☐	☐						
Fairness		5(1)(a)		☐						
Transparency				☐						
Purpose limitation	Specific	5(1)(b)		☐						
	Explicit			☐						
	Legitimate			☐						
	Not further processed			☐						
	(Exceptions)	89(1)		☐						
Data minimisation	Adequate	5(1)(c)		☐						

	Relevant		☐						
	Limited		☐						
Accuracy	Accurate	5(1)(d)	☐						
	Up-to-date		☐						
Storage limitation	Necessary	5(1)(e)	☐						
	(*Exceptions*)	89(1)	☐						
Data security	Integrity and confidentiality	5(1)(f)	☐						
	Security of processing	32	☐						
Data protection by design		25(1)	☐						
Data protection by default		25(2)	☐						

Level 2: Human rights limitation criteria (Article 52(1) CFR) EXTRA

STEP 5 APPRAISAL OF IMPACTS			**STEP 6** RECOMMENDATIONS				
			Response plan, if principle not satisfied				
Criterion	*Satisfied?*	*Explanation*	*Measures in place*	*Measures to introduce*	*Responsible person*	*Priority*	*Deadline*
LEGALITY *Is the envisaged initiative provided for by law of a sufficient quality?*	☐						
ESSENCE *Does the envisaged initiative still make it possible to exercise a fundamental right or freedom?*	☐						
PROPORTIONALITY LEGITIMACY *Does the envisaged initiative serve a legitimate aim?*	☐						
PROPORTIONALITY SUITABILITY *Is the envisaged initiative suited (ever capable) to achieve this aim?*	☐						
PROPORTIONALITY NECESSITY *Is the envisaged initiative necessary to achieve this aim?*	☐						
PROPORTIONALITY PROPORTIONALITY *SENSU STRICTO* (BALANCING) *Is the interference with the right justified in light of the gain in the protection for the competing right or interest?*	☐						

RISK TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

STEP 5 APPRAISAL OF IMPACTS							**STEP 6** RECOMMENDATIONS								
RISK IDENTIFICATION		RISK ANALYSIS					RISK EVALUATION								
							Risk response					*Response plan*			
ID	*Risk*	*Description (risk source, risk owner, etc.)*	*Likelihood [probability] of occurrence* L[P]	*Severity of consequence(s) if risk materialises* S	*Risk level (score)* R = L[P] * S	*Explanation*	*Type*	*Description*	*Revised risk level (score) (Any residual risk?)* L[P]	S	R	*Measures in place*	*Measures to introduce*	*Responsible person*	*Priority*	*Deadline*
1	*[Specify]*															
2																
3																
4																

Risk matrix

Before recommendations	*After recommendations*
[Insert a diagram]	*[Insert a diagram]*

OTHER EVALUATION TECHNIQUES EXTRA

Assessment	*Recommendations*
[Explanation]	*[Explanation]*

RECOMMENDATIONS

	Synthesis of recommendations	*Decision of the controller and its justification*
1	*[Explanation]*	
2		

	Overall recommendation		*Decision of the controller and its justification*
☐	to deploy the initiative without changes		
☐	to modify the initiative	*[Specify how]*	
☐	to cancel the initiative	*[Specify why]*	

COMMENTS

[Explanation]

ONGOING STEPS FOR PHASE II

STEP A STAKEHOLDER INVOLVEMENT

	Stakeholder(s) identified		*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g., opinion)?*	*How was their input included? Why was it rejected?*
internal	Data processor(s)				
	Data protection officer(s) (DPO)				
	Recipient(s) (Article 4(9))				
	Representative(s) (Article 27)				
	Information security officer(s)				
	Legal service				
	Employees, trade unions, contractors, etc.				
	[Other, specify]				
external	Data subjects(s)				
	Representative(s) of data subject(s)				
	Individuals who are not data subjects				
	Representative(s) of individuals who are not data subjects				
	Third parties (Article 4(10))	public sector			
		private sector			
	Experts				
	Supervisory authority(ies) (DPA)				

	[Other, specify]			

Lack of stakeholder involvement in the present phase

[If stakeholders are not involved in the present phase of the DPIA process, explain why.]

STEP B* QUALITY CONTROL

Quality control body	*What feedback was received?*	*How was the feedback implemented? Why was it rejected?*
Data protection officer(s) (DPO)		
Supervisory authority (DPA)		
[Other, specify]		

Lack of quality control in the present phase

[If the quality was not controlled in the present phase of the DPIA process, explain why.]

COMMENTS

[Explanation]

PHASE III: *EX POST* STEPS

STEP 7 PRIOR CONSULTATION WITH A SUPERVISORY AUTHORITY

Objective

The goal of this step is to seek advice from a supervisory authority in case a DPIA process indicates the existence of high residual risk(s) in the absence of measures taken by the controller to mitigate the risk (Article 36).

Implementation

Many DPAs require specific forms (templates) to request a prior consultation; the European Data Protection Board (EDBP) maintains an up-to-date contact list of its Member DPAs.

Insofar as a DPA considers that the envisaged processing operations could infringe the GDPR, it will provide a written notice to the controller within a maximum period of 8 weeks. This period may be extended by 6 weeks depending on the complexity of the request. Should it be necessary, additional information may still be requested from the controller; this will suspend the aforementioned deadlines. A DPA might also use all its powers referred to Article 58.

Competent DPA(s)	
Date of submission	
Date of receipt of the response	
Inquiry (summary)	
Response (summary)	
Decision of the controller after consultation	

COMMENTS

[Explanation]

STEP 8 REVISITING

Objective

The goal of this step is to decide whether and when to perform the DPIA process again, in its entirety or in part, after the envisaged processing operations have been deployed.

Implementation

Following the criteria defined in *Step 3h*, the controller performs a review of a DPIA process when necessary and at least when there is a change in the risk represented by processing operations, i.e., if the nature, scope, context or purpose of the processing operations have changed and hence so has the level of risk (Article 35(11)). A DPIA process has then to be conducted again, in total or in part.

Factors that determine the change in the level of risk vary from a modification of a data processing operation to the context of its deployment to a change in personal data protection law to public pressure.

EXTRA Regardless of the change in the level of risk, the controller may also establish that a DPIA process has to be reviewed regularly (each 6 months, each year, etc.).

	Criterion		*Change?*	*Explanation*
Contextual description	**Nature** *(what types of processing operations? E.g., collection, storage, erasure, etc.)*		☐	
	Scope	Scale (*how much? how many? how far?*)	☐	
		Time (*when? how long?)*	☐	
	Context (*in what circumstances*?)	Internal (*concerning the controller*)	☐	
		External (*concerning individuals, groups, the society, etc.*)	☐	
	Purpose of processing operations, including, when applicable, legitimate interest *(why?)*		☐	
	EXTRA **Benefits** of processing operations	for individuals, including data subjects	☐	
		for the data controller	☐	
		for the society as a whole	☐	

	EXTRA **Drawbacks** of processing operations	for individuals, including data subjects	☐	
		for the data controller	☐	
		for the society as a whole	☐	
Technical description	Categories of personal data *(what?)* ▪ *special categories of personal data* ▪ *personal data of vulnerable people (e.g., children)* ▪ *data of a highly personal nature*		☐	
	Means of processing (infrastructure) *(by what means?)*		☐	
	Envisioned data flows (*where to where? whom to whom?*)		☐	
	Data security *(how is it ensured?)*		☐	
	Jurisdiction/market (*where?*)		☐	
	Actors in the 'supply chain' (*who?*)		☐	
	[Other, specify]		☐	

OVERALL SUGGESTION

What to do with the assessment process?		*When*?	*Decision of the controller and its justification*
☐ revise	☐ entirely	*[Specify]*	
	☐ in part *[Specify]*	*[Specify]*	
☐ do not revise	*[Specify why]*		

COMMENTS

[Explanation]

ONGOING STEPS FOR PHASE III

STEP A STAKEHOLDER INVOLVEMENT

	Stakeholder(s) identified		*What information has been communicated to stakeholders?*	*What input have the stakeholders provided (e.g., opinion)?*	*How was their input included? Why was it rejected?*
internal	Data processor(s)				
	Data protection officer(s) (DPO)				
	Recipient(s) (Article 4(9))				
	Representative(s) (Article 27)				
	Information security officer(s)				
	Legal service				
	Employees, trade unions, contractors, etc.				
	[Other, specify]				
external	Data subjects(s)				
	Representative(s) of data subject(s)				
	Individuals who are not data subjects				
	Representative(s) of individuals who are not data subjects				
	Third parties (Article 4(10))	public sector			
		private sector			
	Experts				
	Supervisory authority(ies) (DPA)				

	[Other, specify]			

Lack of stakeholder involvement in the present phase

[If stakeholders are not involved in the present phase of the DPIA process, explain why.]

STEP B* QUALITY CONTROL

Quality control body	*What feedback was received?*	*How was the feedback implemented? Why was it rejected?*
Data protection officer (DPO)		
Supervisory authority (DPA)		
[Other, specify]		

Lack of quality control in the present phase

[If the quality was not controlled in the present phase of the DPIA process, explain why.]

COMMENTS

[Explanation]

CLOSING PAGE

ENDORSEMENTS

Name	*Role*	*Remarks*	*Signature*	*Date*
	Assessor(s)			
	Data protection officer			
	Data controller(s)			
	[Other, specify]			

STEP C* DOCUMENTATION

Objective

The goal of this ongoing step is to keep intelligible records in writing or another permanent format (analogue or digital) of all activities undertaken within a given assessment process, with due respect for legitimate secrecy.

Implementation

Documentation consists of the present report and the attachments listed below, both drafts and final forms. Assessors also list all the activities undertaken in a given assessment process, e.g., draft versions of the present report or interactions with data subjects, DPAs, etc.

There might be a (national) register of DPIA processes performed to which controllers might be required or recommended to submit a report from a DPIA process.

It is best practice to have (parts of) the present report from a DPIA process as well as all appendices publicly available (e.g., on the website of the controller), with due respect for legitimate secrecy. Once the assessment process is revisited, a new version is to also be made publicly available, with a reference to a previous one.

ACTIVITIES UNDERTAKEN DURING THE PRESENT DPIA PROCESS

Date	*Actor*	*Activity*	*Description*	*Comments*
[Specify]				

ATTACHMENTS

	Attachment	*Confidentiality level*	*Appended?*	*Comments*
Step 1 Step 4	Records of processing activities		☐	
Step 2	Approved codes of conduct		☐	
	Certificates		☐	

	Binding corporate rules (BCR)		☐	
	Standard contractual clauses (SCC)		☐	
	Data protection policies		☐	
	Professional codes of conduct		☐	
	Data sharing agreement(s)	confidential	☐	
Step 3	A copy of a service contract (in case DPIA is outsourced)		☐	
	A list of stakeholders to consult and their contact details	confidential	☐	
	Stakeholder consultation plan		☐	
Step 7	Request for prior consultation with a DPA		☐	
	Response from a supervisory authority		☐	
Step A	Technical briefing(s) for stakeholder consultation		☐	
	Stakeholder consultation (reports)		☐	
	DPO opinion (report)		☐	
	[Reports from other evaluation techniques; specify]		☐	
	[Other, specify]		☐	

COMMENTS

[Explanation]

2 CLOSING REMARKS

In the present Policy Brief, the d.pia.lab has proposed a template for a DPIA process for the EU/EEA, which is based on the interpretation of the relevant legal requirements of the GDPR and reflects best practices for impact assessment. However, nothing in the proposed template is final. It now has to be tested and subsequently revised as experience from its use grows. Therefore, the d.pia.lab continuously seeks feedback on the proposed template to be included in its further revisions, among others.

In parallel, the framework, method and the template do not exhaust the 'architecture' for impact assessment. Further elements, largely of a technical nature, such as a list of possible risks to the rights and freedoms of individuals and a list of possible countermeasures thereto ('knowledge bases'), need to be developed, tested and revised as experience from their use grows. The d.pia.lab will address this in its further work.

SELECTED RELEVANT SOURCES

Margaret Hagan (n.d.), *Law by Design*, https://www.lawbydesign.co.

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* No. 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

Kloza, Dariusz, Niels van Dijk, Simone Casiraghi, Sergi Vazquez Maymir, Sara Roda, Alessia Tanas and Ioulia Konstantinou (2019) "Towards a method for data protection impact assessment: Making sense of GDPR requirements", *d.pia.lab Policy Brief* No. 1/2019, VUB: Brussels. https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf.

Möller, Kai (2012) "Proportionality: Challenging the Critics", *International Journal of Constitutional Law*, 10(3), 709–731. doi: 10.1093/icon/mos024.

Peers, Steve, and Sacha Prechal (2015) "Article 52: Scope and Interpretation of Rights and Principles", in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds.) *The EU Charter of Fundamental Rights: A Commentary*, 1455–1522, Hart Publishing: London. doi: 10.5040/9781849468350.ch-056.

FURTHER READINGS: KEY CONCEPTS

Barak, Aharon (2012) *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press: Cambridge. doi: 10.1017/CBO9781139035293.

Brkan, Maja (2019) "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", *German Law Journal*, 20(6), 864–883. doi: 10.1017/glj.2019.66.

FURTHER READINGS: PRACTICAL GUIDANCE

Agencia Española de Protección de Datos [AEPD] (2018) *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD*, Madrid. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

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.

Commission Nationale de l'Informatique et des Libertés [CNIL] (2018) *Privacy Impact Assessment (PIA) 3: knowledge bases*, Paris. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

European Data Protection Supervisor [EDPS] (2018) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*, Brussels. https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf.

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 (2019) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, Brussels. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

International Association of Privacy Professionals [IAPP] (2020) *2020 Privacy Tech Vendor Report*, Portsmouth, NH. https://iapp.org/resources/article/privacy-tech-vendor-report.

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

ISO (2018) *Information technology – Security techniques – Information security risk management*, ISO 27005:2018, Geneva. https://www.iso.org/standard/75281.html.

ISO (2018) *Security and resilience – Business continuity management systems – Requirements*, ISO 22301:2019, Geneva. https://www.iso.org/standard/75106.html.

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.

Sammut-Bonnici, Tanya, and David Galea (2015) "SWOT Analysis", in: Cary L. Cooper (ed.) *Wiley Encyclopedia of Management*, 1-8, John Wiley & Sons: Chichester. doi: 10.1002/9781118785317.weom120103.

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 ongoing research projects such as PERSONA, HR-RECYCLER and SYSTEM (co-funded by the EU). The views expressed in this Policy Brief do not reflect the views of any of the funding agencies.

We thank, in an alphabetical order, Jonas Breuer, Athena Christofi, Roger Clarke, Katerina Demetzou, Pierre Dewitte, Laura Drechsler, Rossana Ducato, Anna Johnston, Kristoffer Lidén, Gianclaudio Malgieri, Rotem Medzini, Anna Mościbroda, Laurens Naudts, Juraj Sajfert, Mistale Taylor and Heidi Waem for their comments on the earlier drafts of the present Policy Brief.

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