EUROPEAN DATA PROTECTION SUPERVISOR

Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation

v1.1 July 2018

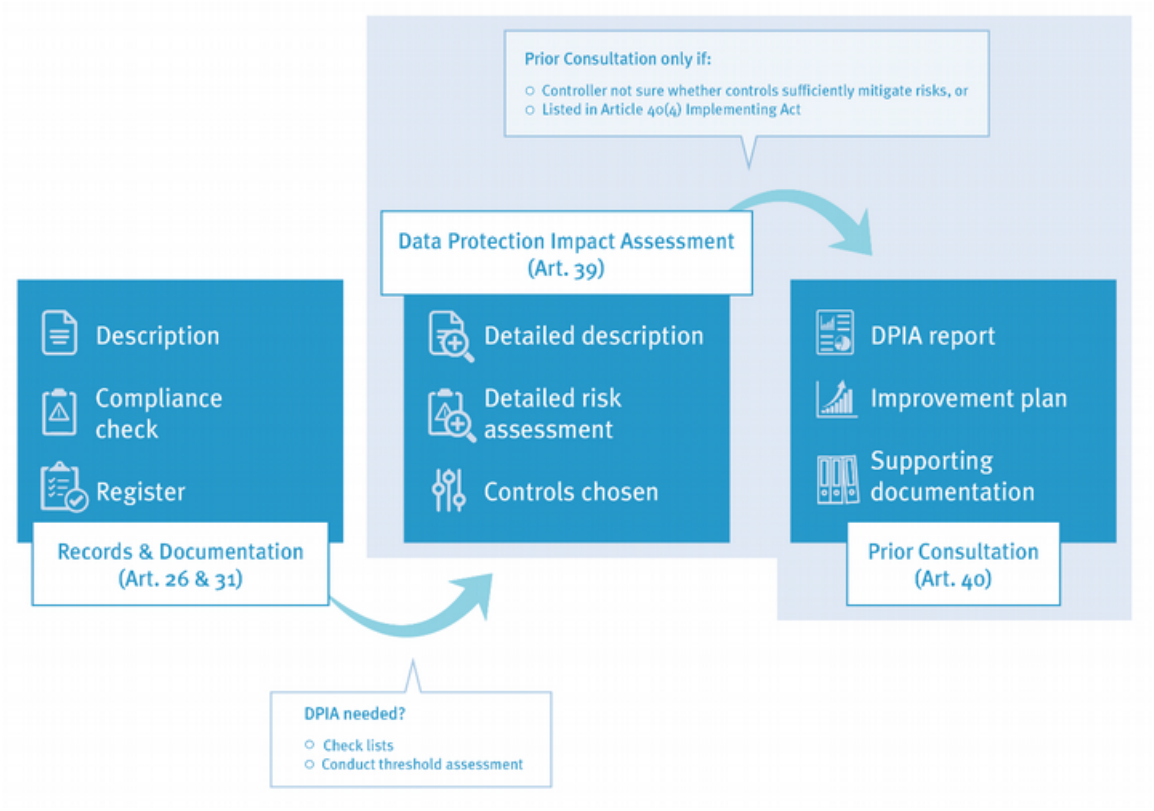
Prior Consultation only if:
Controller not sure whether controls sufficiently mitigate risks, or
Listed in Article 40(4) Implementing Act
Data Protection Impact Assessment (Art. 39)
Description
Compliance check
Register
Records & Documentation (Art. 26 & 31)
Detailed description
Detailed risk assessment
Controls chosen
DPIA report
Improvement plan
Supporting documentation
Prior Consultation (Art. 40)
DPIA needed?
Check lists
Conduct threshold assessment

Table of contents

Table of figures

1. Introduction and scope of Part II

When processing poses 'high risks', you, as person responsible on behalf of the controller, have to analyse and control the risks in more detail using data protection impact assessments (DPIAs). Part II of the *accountability on the ground* toolkit shows you how to do this. In some cases, you may also have to proceed to prior consultation to the EDPS, covered here as well. Part I of the *accountability on the ground* toolkit already showed you how to generate records and related documentation and in which cases you have to do DPIAs.

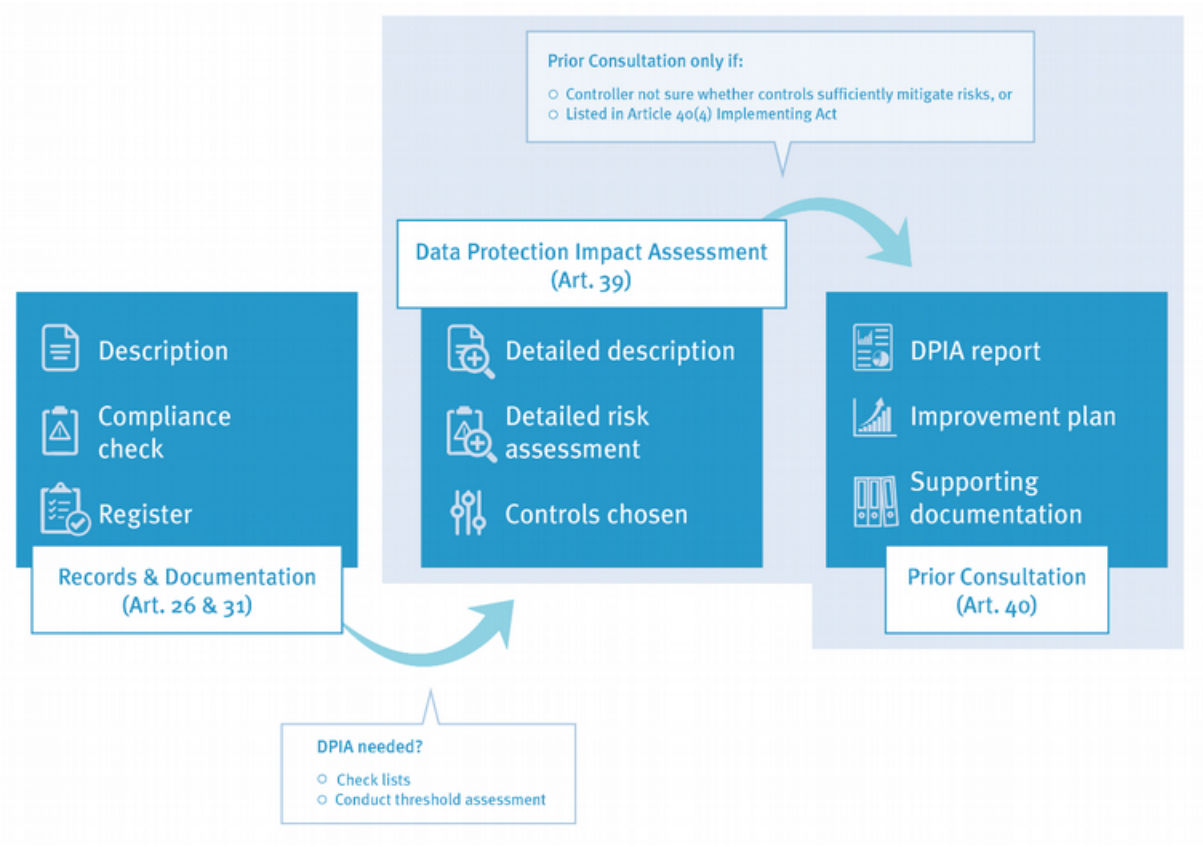

Figure 1: overview of documentation obligations

According to Article 39(1) of the new Regulation[1], 'a single assessment may address a set of similar processing operations that present similar high risks'. Such **'joint' DPIAs may be appropriate when several EUIs implement processing operations in the same way**, e.g. because they have identical rules for specific procedures or because they use the same product in the same way.

If the outcome of the DPIA report is that there are still **high residual risks** (or when the processing is included on a list for mandatory prior consultation), you have to consult the EDPS under Article 40 (see section below).

This document covers the following aspects:

- how to do DPIAs;
- when to send DPIAs to the EDPS for prior consultation;

1 As the new rules are not adopted yet, References to Articles point to the politically agreed compromise between the European Parliament and the Council (Council document 9296/18), unless indicated otherwise. The vote in EP plenary is tentatively scheduled for 10/09/2018..

- who does what in the above processes;
- transition rules from the old Regulation 45/2001 for EU institutions as far as DPIAs and prior consultation are concerned.

For information on how to generate records and how to decide whether you need to do a DPIA, please refer to Part I instead.

2. Responsibilities – who does what?

Accountability means that the controller is in charge of ensuring compliance and being able to demonstrate that compliance. In the EUIs, the controller is legally speaking the 'Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[2] In practice, **top management is accountable for compliance with the rules, but responsibility is usually assumed at a lower level** ('person responsible on behalf of the controller' / 'controller in practice'). The business owner will in many case be the responsible person. You, as the business owner of a process will be the main driver, assisted by the DPO (and DPCs in EUIs which have them)[3].

Should you need to carry out a DPIA, this is according to Article 39 of the Regulation also the controller's task (in practice: top management accountable, business owner responsible), seeking the DPO's advice. The reasoning behind this is that **since it is for controllers to be accountable, they have to own the DPIA process**. On the other hand, DPOs are often the most knowledgeable persons on data protection in an organisation and can be guides and facilitators in the DPIA process.

Responsibility and accountability for the DPIA process lies with controllers, but DPOs may take an important role in guiding them through the process.

For the responsibilities of different roles in your organisation concerning DPIAs, see below:

	Responsible	Accountable	Consulted	Informed
Top Management		X		
Business owner	X			
DPO			X	
IT department			X	
Processors, where relevant			X	
Data subject representatives			(X)	

Figure 2: RACI matrix DPIA process

Top management is accountable for compliance with data protection rules. However, in practice, the business owners of specific processes are likely to do most of the work. As the business owner may rely on other parties, both internal (e.g. the IT department) and external

2 Article 3(1)(8) of the new Regulation

3 There may be cases in which the business owner relies on input from other parties; for example, the head of a business unit for which the IT department develops an application: there may be questions for which the business owner has to seek input from IT, but still, the business owner is responsible for the system.

(e.g. processors or information providers), these have to be consulted and provide their input where necessary. In most cases, the IT department will provide the technical infrastructure and will be best-placed to contribute on information security aspects.

Where appropriate, you also have to consult data subject representatives. Where the processing targets staff members in the EUIs this often means the Staff Committee. Where persons outside your EUI are affected, the controller may need to find solutions to obtain their views as well, where appropriate. This **does not necessarily mean public consultation of all interested parties**. To give an example, think of a system your EUI offers to users in Member States' public administrations and in which personal data of such users are processed - here, you may need to consult representatives of the user base, e.g. via the system's steering committee or similar fora. When consulting, give data subjects' representatives a reasonable deadline to react.

Finally, you should consult your DPO, as the main hub of data protection knowledge in your EUI, throughout the whole process. **Your DPO can serve as a facilitator, keeping in mind that responsibility and accountability finally lie on the controller's side** – DPOs should help controllers to do their job, but should not do it for them.

Please see Annex 1 for a summary of who does what in the steps covered by this part of the toolkit.

3. How to carry out DPIAs?

5.1 Basic requirements for DPIA and choice of methodology

The DPIA process aims at providing assurance that controllers (here represented by you as a person responsible on behalf of the controller / business owner) adequately address privacy and data protection risks of 'risky' processing operations**. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design'** where it is needed the most, i.e. for 'risky' processing operations.

While carrying out the DPIA is your responsibility as business owner of the assessed process, your EUI's DPO can be of help throughout the process - if you need guidance at any stage during the process your EUI's DPO is your first contact point. Also consult your EUI's DPO on each step of the DPIA process.

According to Article 39(6) of the new Regulation, a DPIA shall contain at least:

> '*(a) a systematic description of the envisaged processing operations and the purposes of the processing;*
>
> *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
>
> *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
>
> *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*.'

The **EDPS does not impose a standard methodology for doing DPIAs** on EUIs. However, **any methodology used has to comply with the new Regulation's requirements** and the WP29's guidelines on DPIA[4] interpreting the equivalent provisions of the GDPR, which were endorsed by the EDPB. EUIs are free to use any compliant methodology. Many members of the EDPB already have or will in the future provide DPIA methodologies. Standardisation bodies and industry associations may also develop templates.

For ease of reference, the **EDPS provides an example** for the generic principles for DPIA processes, including a template structure for a report in Annex 3. For some other existing methodologies, see Annex 4, first part.

The EDPS does not impose a specific DPIA methodology on EUIs. You can use any methodology that complies with the rules, the EDPS example provided in this document or another methodology compliant with the WP29/EDPB guidelines.

DPIAs are a **cyclical process**, not a one-off exercise. When you do a DPIA during the development of a new process, it does not stop once the process is adopted and rolled out. If you change the process, your risk environment changes, or simply after a certain period, you have to revisit your DPIA, check if it still reflects reality and update it when required.

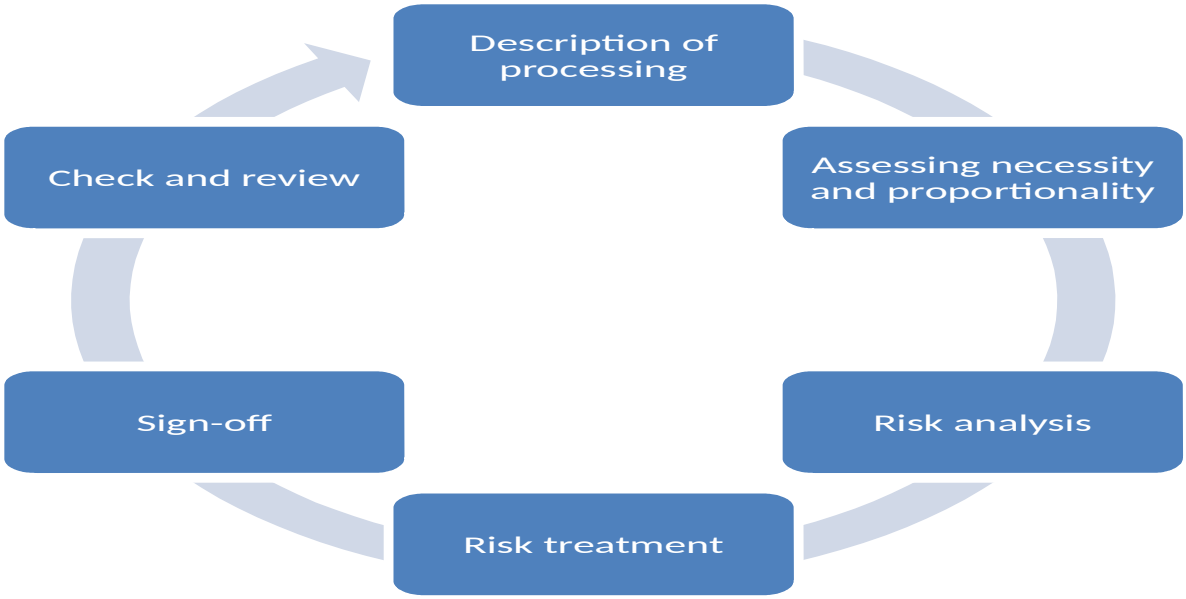

Figure 3: Generic DPIA process

Simply put, you start with a description of your processing – '**What are we doing and how?**' This will be an extended version of the information in the record for this process, including a data flow diagram. Also explain why your organisations needs to carry out this processing operation and how you limit yourselves to what is necessary for the aim of the processing (necessity and proportionality) – '**why do we do this?**' Afterwards, you assess the risks caused by the processing. These are the risks for data subjects – '**How will it affect people when it works according to plan? How will it affect people if things go wrong?**', but also compliance risks for your EUI – '**Are we allowed to do this? Do we comply with specific obligations we may have?**' Then, you choose the appropriate controls for the risks identified – '**What do we do about this?**' All along the way, you document the process and report on it

4 WP248rev.01, http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

– '**…and write it all down'**. Once you reach the end of this first (or any subsequent) cycle of this process, obtain the appropriate management approval. Finally, keep an eye on whether the chosen controls work, whether your environment and/or the process changes – '**Does it work? Does it reflect what we actually do right now?**' – and update your documentation if needed. Annex 3 provides a template structure for such a DPIA report.

3.2 Description of processing

Establishing the context and describing processing operations is the foundation of a solid DPIA process. In short, you have to describe what you plan to and how you plan to do it.

This documentation should allow the reader – be it those affected by the processing, your own top management, who will have to sign off on the DPIA report, the EDPS or other stakeholders – to understand what the processing is about and why you are doing it. While you can of course refer to other documentation your EUI holds, please make sure the description is understandable on its own, since it will serve as one chapter of the DPIA report, which will be a standalone document.

The descriptive part of a DPIA starts from the information in the record, going into more detail and including a detailed data flow diagram.

To create this systematic description of the process, start from the information you already have in your record and add the following points:

- data flow diagram of the process (flowchart): what do we collect from where/whom, what do we do with, where do we keep it, who do we give it to?
- detailed description of the purpose(s) of the processing: explain the process step-by-step, distinguishing between purposes where necessary;
- description of its interactions with other processes - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?
- description of the supporting infrastructure: filing systems, ICT etc.

You may want to use existing documentation of the process or its development to generate this documentation. When you do so, re-read this existing documentation through the lens of "how will this affect the people whose data we process?" and adapt where necessary.

A lot of the information required for the DPIA likely already exists in your EUI, as part of project or process documentation kept for other, non-data protection reasons. You may want to re-use this documentation as far as practicable. However, keep in mind that this other documentation is usually written with a focus on your EUI – 'what does this process mean for our EUI? What does our EUI have to do? How does it affect our EUI?' For the DPIA, the focus is on how the process affects the people whose data your EUI processes – when re-using existing documentation for the DPIA, go through it with this mind-set and be ready to adapt and expand where necessary.

3.3 Assessment of necessity and proportionality

In accordance with Article 39(6)(b) of the new Regulation, you also need to provide an assessment of the necessity and proportionality of the processing. In this section, explain why you plan to do the processing. Be sure to explain that there is a real need for the processing in

order to achieve the aims of the legal basis; the processing effectively addresses this need; and that the processing is the least intrusive alternative (from the perspective of fundamental rights) to achieve this aim (necessity). In addition, you must ensure that the advantages resulting from the processing should not be outweighed by the disadvantages that the processing causes with respect to fundamental rights (proportionality).

In order to do so, explain:

a) Why the proposed processing operations are necessary for your organisation to fulfil the mandate assigned to it. Explain how and why the proposed processing operations are an effective means for your organisation to fulfil its task and whether you considered other alternatives for fulfilling this task, including an explanation for why the approach chosen is the least intrusive one.
b) How the processing is proportionate for the fulfilment of that task. Compare the benefits of the processing against the risks to the fundamental rights posed by the processing. It is possible that a processing that has passed the necessity test, may nevertheless be considered disproportionate.

3.4 Risk assessment

After establishing the context, your next step is to analyse the risks[5] caused by the planned processing in detail. There are two sides to this - the risks to the rights and freedoms of the persons affected and those to your organisation. These are not necessarily the same.

In a DPIA, you assess primarily risks *to the rights and freedoms of data subjects*. At the same time, you should analyse the *compliance risks for your organisation*. These are related, but not necessarily identical.

A 'risk' in this sense is a possible event that could cause harm or loss or affect the ability to achieve objectives. Risks have an *impact* – 'how bad would this be?' and a *likelihood* – 'how likely is this to happen?' Some possible data protection risks are unauthorised disclosures of personal data or inaccurate data leading to unjustified decisions about individuals. This approach is well-known from information security risk management (ISRM) and business continuity planning, only the risks assessed are different – for example, business continuity planning would rather look at risks such as power cuts, flooding and public transport strikes.

The term 'rights and freedoms' of the persons affected refers in the first place to the rights to privacy and data protection (Articles 7 and 8 of the Charter), but also covers related rights that may be impacted as well – e.g. chilling effects on freedom of speech or freedom of assembly due to surveillance measures. This is the assessment referred to in Article 39(6)(c) of the new Regulation.

The risks to your organisation are in the end compliance risks – failing to comply with your EUI's obligations on e.g. informing those whose data you process, or with the requirement to keep data securely may expose your EUI to regulatory action and bad publicity.

In some cases, the risks may differ: unlawfully disclosing medical information would have a reputational costs for your EUI, but would likely not threaten its existence. On the other hand, for the person whose medical information was leaked, the consequences may be graver.

5 The risk screening questions in the records template in Part I refers to the first assessment for determining whether a DPIA may be required. This risk assessment here is about analysing the risks of processes you determined require a DPIA in detail for designing the necessary controls.

Of course, these two kinds of risks are related. Your EUI's specific obligations are in the end controls already chosen by the EU legislator: there's always a risk of data being re-used in unexpected contexts, hence the principle of purpose limitation; processing data without telling those affected about it invades their privacy, hence the obligations for controllers to inform those whose data they process. Additionally, risks to the data subjects in the end also become risks for your organisation: if e.g. user uptake of a new tool is low because of perceived privacy problems, this can affect your organisation's aims for that tool; data breaches and their reputational costs are another obvious example.

While there is a clear ISRM aspect to this (not least since keeping data securely is one of the data protection principles), ISRM is far from all there is to this exercise. ISRM tends to focus on risks that stem from unauthorised system behaviour (e.g. unauthorised disclosure of personal data), while parts of the risks to data subjects and compliance risks stem from the authorised system behaviour for which you do the DPIA.

Processes working exactly as planned may have impacts on data subjects (e.g. employee monitoring). These risks have to be assessed as well, not only the risks of 'things going wrong'. To do so, use the data protection principles as a reference.

For example, the capability of monitoring electricity consumption in real time using smart meters, which allows drawing inferences about private behaviour (Who is home? What are they doing?), is both something persons affected consider as intrusive and an expected consequence of this technology. In a hypothetical example in the EUI, imagine an intrusive case management system tracking all actions and feeding this back in real time to line managers for evaluation purposes and to build profiles of staff (How long have people worked on each single document? How do their turnaround times compare to colleagues? How does their case throughput compare to other colleagues? Who could / should be reassigned to other tasks?). What staff would likely find intrusive about such a hypothetical system is exactly what it is supposed to do.

In all these examples, a classical ISRM approach would likely not address these aspects. While there is a close link to ISRM, since you cannot have good data protection without good information security, the risks to consider here are more than the ones affecting the classic ISRM targets of confidentiality, integrity and availability.

Article 4 of the new Regulation lists the data protection principles[6]. Additional Articles in the new Regulation spell them out in more detail:

6 See Annex 2 of Part I for further explanation.

DP principle	Articles	Recitals
Fairness	*Article 4(1)(a), 17 to 25*	*15, 20, 27, 28, 30-34*
Transparency	*Articles 4(1)(a), 14 to 16, 25*	*15, 28, 29*
Purpose limitation	*Articles 4(1)(b), 6, 13*	*19*
Data minimisation	*Articles 4(1)(c), 12, 13,36*	*15*
Accuracy	*Articles 4(1)(d), 18*	*31*
Storage limitation	*Articles 4(1)(e), 13*	*15, 26*
Security	*Articles 4(1)(f), 33*	*38*

Figure 4: data protection principles in the new Regulation

Go through your data flow diagram and for each step, ask yourself how this could affect the persons concerned against the background of the data protection principles.

Using the guiding questions further below as a starting point, think about what could affect the attainment of these goals and what the possible impact on the persons affected could be, assessing severity and likelihood. For the scale to be used for this assessment, there are no specific requirements, but you may want to use scales your internal stakeholders are familiar with, e.g. because you use them in your ISRM process or in other risk management exercises. Most EUIs use a 5-point scale ranging from 'very low' to 'very high'. To be able to have a consistent risk evaluation, define what each step of the scale means, e.g. in terms of reputational or financial impact or frequency for the likelihood. For example, disclosing medical data to persons without a need to know will likely have higher impact than disclosing contact information of EUI staff; a disclosure to unauthorised staff within your EUI may have less impact than accidental disclosure to the public at large.

For this exercise, walk through your data flow diagram and ask yourself for each step how this could affect these targets. Some targets are more relevant for some kinds of processing steps than others. The table below maps the targets to some generic processing steps, indicating the most relevant targets for each. These are the minimum aspects to check.

	Fairness	Transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Security
Collection	***X***	***X***	***X***	***X***	***X***		***X***
Merging datasets	***X***	***X***	***X***	***X***	***X***		***X***
Organisation/structuring			***X***	***X***	***X***		
Retrieval/consultation/use	***X***	***X***	***X***		***X***	***X***	***X***
Editing/alteration		***X***		***X***	***X***		***X***
Disclosure/Transfer	***X***	***X***	***X***	***X***	***X***		***X***
Restriction			***X***	***X***	***X***	***X***	***X***
Storage	***X***	***X***	***X***			***X***	***X***
Erasure/destruction			***X***			***X***	***X***

Figure 5: mapping data flow diagram items and protection targets

For this risk assessment, go through your data flow diagram and ask yourself for each step how this could affect the protection targets / data protection principles, starting from the guiding questions below.

3.5 Guiding questions on data protection principles

Use the guiding questions below as a starting point both for analysing the specific steps and for the overall assessment. Not all questions will be relevant for all steps and sometimes, you will need to go into more detail.

'Fairness' of the processing has several aspects: is the processing **unexpected** for the persons 'affected? Does it have **chilling effects** on the exercise of their other rights, making people less likely to exercise them? How can they **intervene** and make their voice heard?

Is the processing **unexpected** for data subjects, e.g. because you are re-using data for a different purpose than the one they were initially collected for, or because two formerly separate databases were merged or interconnected by new legislation? Even if data subjects don't read the privacy statement, would they expect this to happen?

In case you rely on consent, make sure that it is valid, free and informed, as otherwise your processing may become unlawful and unfair (e.g. when people consent to one thing and you do another).

Thirdly, ask yourself if the processing operations you plan could generate **chilling effects** on the exercise of their other rights. 'Chilling effects' decrease the likelihood that people exercise their fundamental rights. As an example, think CCTV in a publicly accessible area outside your EUI's entrance and how it may affect freedom of assembly and speech there.

The third aspect of fairness, 'ensuring persons' rights to intervene' refers collectively to the rights of access, rectification, erasure, restriction of processing, objection and data portability

people have under the new Regulation. They need to be able to receive a copy of the data you hold about them; to have it corrected if it is incorrect; to have it erased if you keep it unlawfully; to have its processing restricted under certain circumstances (e.g. by limiting its visibility to certain staff members); to object to processing on grounds relating to their particular situation; and in some cases to obtain data portability.

If people are not able e.g. to rectify incorrect information in time, this could have negative effects on them. You have to ensure that persons affected can exercise these rights under the new Regulation without affecting your EUI's operations.

This means for example designing systems in a way that you can restrict/block specific entries of a database without affecting its operation or allowing people to easily access and export their personal data held in a system. You should make it easy for people to exercise their rights – provide easy-to-find information on contact points and communicate requirements upfront (e.g. how individuals can demonstrate that they really are the data subject when requesting access). For more information on all of these rights, see guidelines on the rights of individuals[7].

Guiding Questions on fairness

1. Can people expect this to happen, even if they don't read the information you provide them with?
2. In case you rely on consent, is it really freely given? How do you document that people gave it? How can they revoke their consent?
3. Could this generate chilling effects?
4. Could this lead to discrimination?
5. Is it easy for people to exercise their rights to access, rectification, erasure etc.?

Figure 6: Guiding questions on fairness

'Transparency' is grouped with fairness in Article 4(1)(a). It means that the people whose data you process have to know that you do so and be able to understand what you do with their data and why (Articles 14 to 16 of the new Regulation). This is especially important if you do not collect the data directly from the persons affected, but from other sources. In case you have a legal reason not to inform people (or to not inform them just yet - e.g. the early stages of an OLAF investigation), you have to think about when and how you will be able to inform them.[8]

If people do not know about your processing of their personal data, they cannot exercise their other rights under the new Regulation; additionally, if your processing relies on consent, not informing people appropriately means that their consent is invalid. For more information, see the EDPS Guidance on Articles 14 to 16 of the new Regulation.[9]

Guiding Questions on transparency

1. How do you make sure that the information you provide actually reaches the individuals concerned?
2. Is the information you provide complete and easy to understand?
3. Is it targeted to the audience? E.g. children may require tailored information
4. In case you defer informing people, how do you justify this?

7 https://edps.europa.eu/data-protection/our-work/publications/guidelines/rights-individuals_en
8 The exact extent to which EUIs will be able to restrict these rights will also depend on the outcome of the legislative process.
9 https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf

Figure 7: Guiding questions on transparency

‘**Purpose limitation’** in Article 4(1)(b) is the principle that personal data collected for one purpose should not be re-used for other, incompatible purposes. EUIs can safeguard this principle both by business rules and by the design of systems and processes themselves. An important design feature that can often be helpful here is ‘unlinkability’. This concept refers to the property of not being (easily) able to link personal data to other information about the same person. This helps to enforce purpose limitation and, for example, helps prevent the creation of comprehensive profiles of individuals for purposes that they would not have expected.

Archiving, scientific research, historical or statistical purposes may be considered compatible, but require some safeguards. If you want to keep / make available personal data for such purposes, think about how this could affect people and how to minimise this risk. Examples could be aggregating data (birth dates to age groups) or delaying disclosure (opening of archives).

Purpose limitation acts as a stop against function creep. Imagine a hypothetical situation in which staff members receive confidential career counselling, mentioning that they’d like to move jobs and this information being re-used to deny them training as they may soon leave the organisation. This would be a clear infringement of the purpose limitation principle.

Guiding Questions on purpose limitation

1. Have you identified all purposes of your process?
2. Are all purposes compatible with the initial purpose?
3. Is there a risk that the data could be reused for other purposes (function creep)?
4. How can you ensure that data are only used for their defined purposes?
5. In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Figure 8: Guiding questions on purpose limitation

‘Data minimisation’ means that your EUI only processes the personal data it really needs to fulfil the purpose of the processing and only keeps them for as long as necessary for this purpose. This is also key for avoiding unlawful excessive processing of personal data.

This means for example ensuring that you only request the necessary information in forms and that you do not keep personal data ‘just in case’ you may find a use for them later. Specific risks here could be e.g. default settings in commercial off-the-shelf software resulting in the processing of personal data not actually required for your purposes. It also means thinking about whether the data you want to collect actually give you the information you want to obtain - do the data measure what you intend to measure?

In case you plan to make personal data available for archiving, scientific research, historical or statistical purposes unrelated to the business purpose, think about how this could affect data subjects and minimise this impact. If you can fulfil these purposes in ways that do not involve personal data (e.g. only keeping statistical outputs, but not the micro-data), do it that way. If it is necessary to keep (some) personal data for these purposes, think about how you can minimise them (e.g. keeping age ranges instead of birth dates or otherwise aggregating data).

Guiding Questions on data minimisation

1. Do the data you collect measure what you intend to measure?
2. Are there data items you could remove (or mask/hide) without compromising the purpose of the process?
3. Do you clearly distinguish between mandatory and optional items in forms?
4. In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Figure 9: Guiding questions on data minimisation

'Accuracy' means that your EUI is obliged to make sure that the information it processes about people is accurate (Article 4(1)(d) of the new Regulation) – taking action based on inaccurate information may negatively affect people and expose your EUI to liability. If your EUI realises information is inaccurate or incomplete, it has to rectify[10] or erase it without delay. Providing easy means for data subject access can help here. In some processing operations, the factual accuracy of statements may be in dispute between the parties affected (e.g. a whistle-blower's accusations). In such cases, 'accuracy' refers to the fact that a certain statement (containing personal data) has been made and that it is accurately recorded; the other party should be able to complement the information recorded and provide its own view on the matter.[11]

Guiding Questions on accuracy

1. Are the data of sufficient quality for the purpose?
2. What could be the consequences for the persons affected of acting on inaccurate information in this process?
3. How do you ensure that the data you collect yourself are accurate?
4. How do you ensure that data you obtain from third parties are accurate?
5. Do your tools allow updating / correcting data where necessary?
6. Do your tools allow consistency checks?[12]

Figure 10: Guiding questions on accuracy

'Storage limitation' in Article 4(1)(e) of the new Regulation refers to keeping personal data 'as long as necessary and as short as possible'. In some cases, EU legislation will lay down conservation periods for specific processing operations, while in others, the periods will be for your EUI to determine. Establish your conservation periods from your business needs for the specific process – this is not a technical question, it's a business question. In the first place, this is about the administrative retention period, but think also about your post-retention action in case of archiving.

In case you want to keep (parts of) the data for archiving, scientific research, historical or statistical purposes unrelated to the business purpose, think about how this could affect data subjects (see also 'purpose limitation' above). Be aware that the new Regulation does not provide a blanket permission to store everything for an extended period of time for archiving, scientific research, historical or statistical purposes. In each case, you must have an appropriate legal basis for the processing and assess the necessity and proportionality of any

10 Changes made for rectifying personal data should be auditable, no to affect the integrity of the data.

11 To give another example: a staff member disagrees with negative feedback from her line manager in an appraisal procedure. The line manager's statement is 'accurate' in the sense that it is the line manager's assessment. Nonetheless, staff should be able to provide their own view and to challenge negative reports in an appeals procedure. If the report is changed on appeal, this is however not "rectification" in the sense of Article 14 of the new Regulation.

12 e.g. automatically checking if birth dates entered are in the right format and in a plausible range.

data storage. In addition, you must also think of safeguards you can apply – e.g. aggregating personal data kept/disclosed for research purposes, banning re-identification in the conditions for granting access for research purposes, etc.

You will find guidance on conservation periods in many of the EDPS guidelines on specific processing operations.[13]

Guiding Questions on storage limitation

1. Does EU legislation define storage periods for your process?
2. How long do you need to keep which data? For which purpose(s)?
3. Can you distinguish storage periods for different parts of the data?
4. If you cannot delete the data just yet, can you restrict access to it?
5. Will your tools allow automated permanent erasure at the end of the storage period?

Figure 11: Guiding questions on storage limitation

'Security' in Article 4(1)(f) refers back to concepts of 'confidentiality' and 'integrity', well-known from ISRM. 'Confidentiality' refers to the property of information only being available to authorised persons with a need to know. 'Integrity' refers to the property of information not being able to be changed without proper authorisation.[14] The third part of the ISRM triad, availability, is not included in the list in Article 4(1)(f), but Article 33(1)(c) stresses the need to restore the 'availability' of the data, thus including also this essential dimension of information security.

Breaches of confidentiality of personal data can cause various kinds of harm, such as psychological distress (e.g. a leak of medical data) and financial harm (e.g. when leaked personal data are used for identity theft) to individuals. To avoid this, you should design your systems in a way that access to personal data is limited on a strict need-to-know basis and that personal data are protected against being read by unauthorised person at all stages – whether at rest or in transit, using encryption where appropriate. Logging accesses to personal data is a way to ensure that you spot any possible breaches and to show proof of who accessed the data.

Breaches of integrity of personal data can affect people if decisions about them are taken on the basis of corrupted information. To avoid this, you have to for example design your systems in a way that personal data can only be changed by authorised users and that such changes are auditable.

Breaches of availability prevent the very use of the data. This can also affect the persons concerned (e.g. not possible to pay salaries if the data are not accessible or the system is down) and the exercise of data subjects' rights (access, rectification, etc.).

For this target, see also the guidance on security measures for personal data processing[15]. Your organisation should also have a developed approach on how to manage information security in general, which will also benefit data protection.

Guiding Questions on security

1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks potentially affecting personal data and the IT systems

13 https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en
14 If information can be changed, such changes have to be auditable.
15 https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en

supporting their processing?
2. Do you target the impact on people's fundamental rights, freedoms and interests and not only on the risks to the organisation?
3. Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
4. Do you manage your system vulnerabilities and threats for your data and systems?
5. Do you have resources and staff with assigned roles to perform the risk assessment?
6. Do you systematically review and update the security measures in relation to the context of the processing and the risks?

Figure 12: Guiding questions on security

After having gone through the data flow diagram this way, take stock of the risks identified and ask yourself whether there may be horizontal risks in the processing that you cannot easily link to a specific processing step. Make sure you catch these kinds of risk, too – sometimes the whole is more than the sum of its parts.

These questions are only a starting point, but should help you to zero in on problematic aspects of planned processing operations.

Once you are finished with this stage, document your results in the DPIA documentation. The higher the risk, the more thought should go into devising controls in the next step.

3.6 Risk treatment

Once you have established the risks, you have to choose appropriate mitigating measures (controls). This sections describes possible approaches to minimising risks and provides some generic controls.

Please note that while the shift towards a 'risk-based approach' in the GDPR and the new Regulation is one important feature of the new rules, there is still a certain floor of specific requirements to ensure compliance, which your organisation cannot fall below without exposing itself to regulatory action. Put differently: there are risks that your organisations must not simply accept, but will have to mitigate or avoid. Think of these as mandatory controls included by the legislator because they are always a good idea. This concerns especially the protection target fairness. Your EUI cannot say 'we won't provide access, it's too much of a hassle', but your EUI may be able to say –when appropriate– that 'given the few requests we expect in this new system, we will not invest in an automated self-service system for people to obtain access, but will only provide a contact point and deal with requests manually when they come in'.

When selecting the controls/mitigating measures, compliance with the new Regulation is the minimum standard you cannot go below.

Controls may target likelihood (example: awareness raising for HR staff will decrease the likelihood of them disclosing information to unauthorised parties, but does not affect the impact when it happens), impact (example: making sure that storage devices are encrypted reduces the impact of a USB stick with personal data left on a train, but not the likelihood of this happening), or both. In some cases, you may also be able to avoid risks completely

(example: a process re-design removes the need for personal data – data you do not hold cannot be unlawfully disclosed).

You can design controls from scratch, or also take inspiration from good practice catalogues, such as general and subject specific guidance provided by the EDPS[16] and other DPAs; guidance from national European and international standard organisations such as BSI, CEN/CENELEC/ETSI and ISO; guidance from information security organisations and projects such as ENISA and OWASP; guidance from academic work, EU co-funded research projects and security and privacy engineering initiatives such as the Internet Privacy Engineering Network[17], and your organisation's own information security rules. Make sure that the controls chosen comply with the new Regulation.

By way of example, here are some generic controls grouped by how they help to control risks:

- Preventative: prevent risks from materialising, e.g.:
  - raising awareness among staff to prevent unauthorised data sharing;
  - keeping conservation periods and the amount of data collected to the minimum, so that there are less data that could possibly leak and that temptation for purpose changes after the fact is lowered;
  - user management to quickly deactivate access rights of persons who no longer have a need to know (e.g. because they changed jobs);
  - segregating personal data so that breaches of confidentiality in one repository do not affect others;
- Detective: monitor your processing operations in order to ensure that you quickly notice breaches, e.g.:
  - logging operations and self-monitor to detect data breaches or illicit use;
  - keeping track of when and how you informed people about the processing;
- Repressive: ensure that you have means in place to quickly end detected breaches, e.g.:
  - procedures to correct inaccurate data;
  - certificate revocation mechanisms to stop the use of compromised credentials;
- Corrective: ensure that you have the means to undo or limit damage after the fact, e.g.:
  - keeping backups, so you can revert to the status quo ante after systems have been compromised;
  - informing recipients after an unauthorised transfer and instructing them to delete the data;

Please find below a few examples of controls, grouped by protection target. As the risks and therefore the controls to be adopted depend on the specific processing operations for which you do a DPIA, these can only be a starting point.

Target	Generic controls
Fairness	• check allowed/expected use when re-using datasets
Transparency	• automatically notifying data subjects
Purpose limitation	• Limiting export functionalities

16 Always to be verified against the specific context - EDPS guidelines give general recommendations; how they can be applied in your organisation may depend on the specificities of the process.

17 For further information and an information repository, see: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

	• Avoiding generic identifiers
Data minimisation	• collecting age ranges instead of birth dates
Accuracy	• consistency checks • data quality reviews
Storage limitation	• distinguishing between conservation period for different parts of data, restricting access to relevant profiles
Security	• refer to your EUI's ISRM framework

Figure 13: Indicative list of generic controls per target

Choose the controls necessary to ensure compliance and appropriately mitigate the risks.

If you find that improvements are needed to mitigate risks down to an acceptable level, create an improvement plan with the improvements determined to be necessary and timescales for implementing them.

3.7 Documentation and reporting

The DPIA process helps you to think through the privacy and data protection implications of processing operations. In order to be able to prove that you have gone through this process, you need to document it.

The main deliverable of the DPIA process is the DPIA report summarising the findings from this section. See Annex 3 for a template for a DPIA report.

The DPIA report is the main deliverable of the DPIA process.

3.8 Review cycles

DPIAs are a process, not a one-off exercise. In this way, they are similar to other management processes like ISRM.

Choose the length of the review cycle based on the risks posed by your processing operations. The higher the risks, the shorter the review cycle should be. The choice of cycle length is for the controller to make. Per default, the EDPS recommends a review cycle of 2 years, with an extraordinary review in case of significant changes to the processing operations. There may be other circumstances requiring an extraordinary review as well, such as significant data breaches showing that your EUI's security controls may not be up to the task. Smaller changes, such as improved security controls following the continuous improvement process for your services, do not necessarily require an update of the DPIA: check whether the DPIA still fits your actual risk treatment and update if need be.[18]

You may want to synchronise these review cycles with other regular reviews of relevant processes and their documentation (e.g. ISRM or internal control measures).

18 Example: one of your organisational controls against breaches of confidentiality is having users of a system sign confidentiality declarations. You update the text of the declaration to be stronger. This does not seem to require an update of the DPIA report.

Review DPIA reports on a regular basis (suggested: every two years) and prepare for extraordinary reviews where needed.

3.9 Publicity of DPIA reports

The new Regulation does not specifically require publication of DPIA reports. That said, the EDPS considers publication of DPIA reports to be a good practice. You should strive to at least publish a summary of the report. Parts of the reports that should not be disclosed to the public, e.g. details on security measures, can be removed where appropriate.[19]

You may want to document your DPIA process in a way that public (or publishable) parts of the documentation can easily be differentiated from those that should remain internal. The template for a DPIA report in Annex 3 is structured in a way that you can easily pick and choose which parts to publish and which to keep internal.

Publication also helps to reassure your stakeholders and the public at large that your EUI complies with the rules on data protection, fostering trust and showing that EUIs lead by example when it comes to complying with fundamental rights. Good places to publish DPIA reports would be your public register and the part of your EUI's website explaining the policy supported by the processing operations.

'Do good things and talk about them' – It is a good practice to publish your DPIA reports, at least in summary form. Publication allows showcasing the work that has gone into making processing operations compliant and can foster trust with your stakeholders and the public at large.

4. When to do a prior consultation?

Only some processing operations requiring a DPIA will additionally require prior consultation to the EDPS. Prior consultation is for 'grey' cases where you are not sure that you have appropriately mitigated the risks, but which are not so clear-cut that the only option would be to abandon the project. Should you find yourself in such a situation, consult your DPO.

Article 40(1) of the new Regulation states that prior consultation is required when a DPIA 'indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation'. In this case, the controller – after consulting the DPO – has to consult the EDPS.[20] As the name implies, this consultation has to take place prior to the start of processing operations.

In line with the WP29 DPIA Guidelines, not all processing operations requiring DPIAs will also require prior consultation.

19 Please note that as a document held by your EUI, the full DPIA documentation may be requested under Regulation (EC) 1049/2001 on public access.

20 Article 39 of Regulation (EU) 2016/794 imposes a specific obligation for 'prior consultation' of the EDPS on Europol. This is a different obligation with different criteria triggering it.

1. There are cases in which following a DPIA and the (additional) controls implemented, risks will be appropriately mitigated to an acceptable level. Such cases do not require prior consultation.
2. There may also be cases where, following the DPIA, you realise that risks cannot be mitigated to an acceptable level. In such cases, you should abandon the project if it proves impossible to implement in a compliant way.
3. There will be cases in which you see that improvements are necessary to mitigate the risks to an acceptable level and you currently have "high residual risks". These "grey" cases are what prior consultation is for.

Independently of the above, the European Commission may, under Article 40(4) of the new Regulation, adopt implementing acts requiring prior consultation for specific cases of processing operations for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health. So far, the European Commission has not done so.

See below for an overview of the relationship between the 'records of processing' (Article 31), DPIAs (Article 39) and prior consultation (Article 40). All processing operations require records; some of them will require a DPIA; and some of those may require prior consultation.

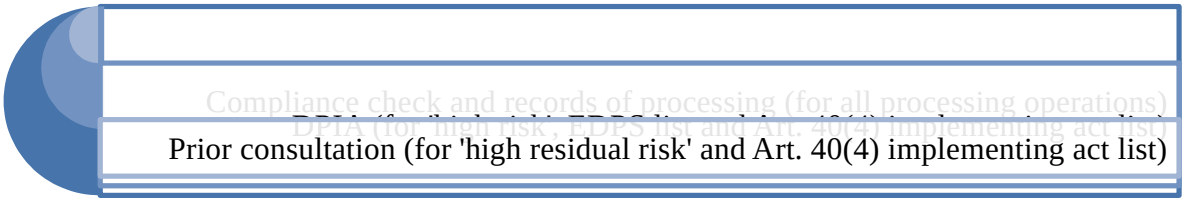

Figure 14: Relationship records - DPIA - prior consultation

When you submit a prior consultation, the EDPS will analyse the documentation submitted and provide guidance on any improvements necessary.

The documentation to be included in the request for prior consultation will essentially be the DPIA report.[21] Please provide the following documentation:

- the record and the full DPIA report;
- treatment plan explaining the planned improvements to the controls;
- related documentation of your ISRM process;
- any other documentation you deem necessary for understanding the risks posed by the planned processing and the choice of controls.

Following receipt of a prior consultation, the EDPS will provide recommendations to ensure compliance.

According to Article 40 of the new Regulation, the deadline for the EDPS to provide recommendations is eight weeks from receipt of the prior consultation, not counting suspensions for requests for further information. For complex cases, this period may be extended for another six weeks within one month of receipt of the notification. The EDPS will inform controllers (and processors, where relevant) of this extension and provide reasons. The lack of a reply by the EPDS within this deadline does not affect possible later interventions by the EDPS (see recital 48 of the new Regulation).

21 The items mentioned in Article 40(3) points (a) to (c) will be included in the DPIA report anyway; item (d) is known to the EDPS anyway.

Under Article 27 of the old Regulation, you had to notify certain 'risky' processing operations to the EDPS for prior checking. There are however some important differences between the former prior checking and prior consultations under the new Regulation:

- different standards for triggering it: residual risk instead of gross risk;
- lack of a reply does not imply approval.

The different criteria will mean that there will be fewer prior consultations than there were prior checks.

5. How to get ready?

As a person responsible on behalf of the controller, you will not have to create your documentation from zero. EUIs already carry out processing operations that will trigger the criteria for conducting DPIAs. Many of these have been prior-checked under Article 27 of the old Regulation. While the criteria for prior checking under the old Regulation and the new Regulation are not identical, there is a certain overlap – most processing operations requiring a DPIA under the new Regulation already required prior checking under the old Regulation. There are also processing operations that required prior checking under the old Regulation, but which will not require a DPIA.

When preparing for the new Regulation, check your EUI's past prior checking cases - some of these may also require a DPIA.

Please see below for information on how to deal with existing processing operations that may possibly require a DPIA:

(i) Closed prior checking cases

Processing operations that will require a DPIA and that have been prior-checked with a positive result (with a closed follow-up procedure, where applicable) under the old Regulation can benefit from a grace period of 2 years, so no DPIA will be necessary immediately.

However, if/when procedures and/or risks change, a DPIA will be necessary in order to verify compliance with the new Regulation.

(ii) Prior checking Opinions still in follow up phase:

If follow-up for processing operations that required prior checking under Article 27 of the old Regulation and a DPIA under the new Regulation is still ongoing, you should try to have it closed before the new rules become applicable. That way, you will have a clean slate. If follow-up is still ongoing by the time the new Regulation will become applicable, you should check if a DPIA is needed by conducting a threshold assessment [see Part I - Section 4] and if this confirms the need for a DPIA, start carrying it out immediately.

6. Conclusion

Part II of the *accountability toolkit* provided you with practical guidance on how to carry out DPIAs and when you additionally will have to go for prior consultation to the EDPS.

As business owner, you are in the driver's seat – data protection compliance is your responsibility. Your DPO will be your guide, but choosing and implementing the concrete measures to ensure compliance is your responsibility.

DPIAs are an important tool for managing the privacy and data protection risks for your 'riskier' processing operations. Going through the process provides evidence that you thought about these risks and chose justifiable means for managing them. When the EDPS checks how your EUI complies with its data protection obligations, you can be sure that we will have a look at your DPIAs. Failure to do DPIAs when required may result in an administrative fine against your EUI.[22]

For particularly difficult cases, you proceed to prior consultation to the EDPS; when replying, the EDPS will give further guidance on how to ensure compliance with data protection rules. In keeping with the 'accountability' spirit of the new Regulation, we do not expect that there will be many prior consultations. Definitely, we expect that there will be fewer prior consultations than prior check notifications under the old Regulation.

22 Article 66 of the new Regulation.

Annexes

1. Who does what?

The list below provides a quick overview of "who does what?" delineating what is for the controllers / business owner to do and what for DPOs.

Controller / business owner:

- draft DPIAs;
- analyse whether you need to continue to prior consultation.

DPO:

- guide controllers through DPIA process;
- provide feedback on draft documentation/DPIAs;
- reply to consultations from controllers / business owners;
- provide liaison point between EUI and EDPS, including submitting prior consultations.

Other functions (such as IT or legal)

- support controller/business owner and DPO as needed.

2. Catalogue of guiding questions per data protection principle

Guiding Questions on fairness

1. Can people expect this to happen, also if they don't read the information you provide them with?
2. In case you rely on consent, is it really free? How do you document that people gave it? How can they revoke their consent?
3. Could this generate chilling effects?
4. Could this lead to discrimination?
5. Is it easy for people to exercise their rights to access, rectification, erasure etc.?

Guiding Questions on transparency

1. How do you make sure that the information you provide actually reaches the individuals concerned?
2. Is the information you provide complete and easy to understand?
3. Is it targeted to the audience? E.g. children may require tailored information
4. In case you defer informing people, how do you justify this?

Guiding Questions on purpose limitation

1. Have you identified all purposes of your process?
2. Are all purposes compatible with the initial purpose?
3. Is there a risk that the data could be reused for other purposes (function creep)?
4. How can you ensure that data are only used for their defined purposes?
5. In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Guiding Questions on data minimisation

1. Are the data of sufficient quality for the purpose?
2. Do the data you collect measure what you intend to measure?
3. Are there data items you could remove (or mask/hide) without compromising the purpose of the process?
4. Do you clearly distinguish between mandatory and optional items in forms?
5. In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Guiding Questions on accuracy

1. What could be the consequences for the persons affected of acting on inaccurate information in this process?
2. How do you ensure that the data you collect yourself are accurate?
3. How do you ensure that data you obtain from third parties are accurate?
4. Do your tools allow updating / correcting data where necessary?
5. Do your tools allow consistency checks?

Guiding Questions on storage limitation

1. Does EU legislation define storage periods for your process?
2. How long do you need to keep which data? For which purpose(s)?
3. Can you distinguish storage periods for different parts of the data?
4. If you cannot delete the data just yet, can you restrict access to it?
5. Will your tools allow automated permanent erasure at the end of the storage period?

Guiding Questions on security

1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks possibly affecting personal data and the IT systems supporting their processing?
2. Do you target the impact on people's fundamental rights, freedoms and interests and not only the risks to the organisation?
3. Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
4. Do you manage your system vulnerabilities and threats for your data and systems?
5. Do you have resources and staff with assigned roles to perform the risk assessment?
6. Do you systematically review and update the security measures in relation to the context of the processing and the risks?

3. Template structure of DPIA report

The structure below can provide a template for a DPIA report.

1. **Project name**
2. **Validation/sign-off**

   Approval chain and sign-off

3. **Review**

   Provide information on review cycle, current status and versioning information for previous iterations

4. **Summary**

   Provide a short overview of the main findings of the DPIA: main risks identified, controls chosen…

5. **Reason for this DPIA**

   Quickly explain: (a) listed in positive list or (b) outcome of threshold assessment

6. **Main actors involved**

   Provide an overview of who was involved when on which parts

7. **Description of processing**

   Starting from the information in the record for the processing operation, prepare the following:

   - *data flow diagram of the process (flowchart): what do we collect from where/whom, what do we do with, where do we keep it, who do we give it to?*
   - *detailed description of the purpose(s) of the processing: explain the process step-by-step, distinguishing between purposes where necessary,*
   - *description of its interactions with other processes - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?*
   - *description of the supporting infrastructure: filing systems, ICT etc.*

8. **Necessity and proportionality**

   Starting from the information in the record for the processing operation, explain the following:

   - *why are the proposed processing operations necessary for your EUI to fulfil the mandate assigned to it?*
   - *does the processing stay inside what is proportionate for the fulfilment of that task?*

9. **Analysis of risks and establishment of controls for identified risks**

   You may refer to the list in Annex 2 as a starting point

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity (gross)	Likelihood (gross)	Controls	Severity (residual)	Likelihood (residual)
1	Electronic repository of personal files	Unauthorised secondary use	Purpose limitation, Security	3	3	Staff receive DP training. Access control list limits access to those with need to know. Accesses are logged and logs analysed; see points A, B, C of EUI Security Policy XYZ.	3	1
2	Electronic repository of personal files	Corruption of data	Data quality, security	4	1	Changes are logged and backups kept	1	1
…								
n								

10. DS comments (if applicable)

Who did you consult? What were their comments and concerns? How did you integrate them (e.g. by adding additional risks in section 7 above)?

11. DPO comments

What were DPO's comments and concerns? How did you integrate them (e.g. by adding additional risks in section 5 above)?

4. Reference documents

4.1. Other DPIA methodologies by EDPB members

If you do not want to use the methodology proposed in this document, you are free to use any of the methodologies below in this section, provided they are updated where necessary to be GDPR/new Regulation-compliant:

- Belgian Privacy Commission: DPIA GL (FR/NL)
- Denmark Datatilsynet – Konsekvensanalyse (March 2018)
- Germany (Datenschutzkonferenz): Standard Data Protection Model, V.1.0 – Trial version, Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016: DE / EN

- Spanish Data Protection Agency - Guía práctica de Evaluaciones de impacto (2018)
- French CNIL
    - DPIA software tool (updated 2018)
    - CNIL Privacy Impact Assessment Manuals 1 (Methodology), 2 (Tools: templates & knowledge bases) & 3 (Good Practices) of July 2015
- Slovenian DPA: Smernice ocene učinkov na varstvo osebnih podatkov (2018)
- UK Information Commissioner Data Protection Impact Assessments (May 2018)

4.2. Other (D)PIA methodologies by third parties

These methodologies have been adopted by other third parties, such as data protection authorities in third countries. They may not comply with the standards set out in GDPR/"new 45" and are included for background information only:

- Australian Information Commissioner - Guide to undertaking privacy impact assessment (May 2014)
- Canadian Privacy Commissioner - Guide for submitting privacy impact assessment (March 2011)
- New Zealand's Privacy Commissioner (2015) - Privacy Impact Assessment Toolkit
- USA DHS - PIA guidance & template (June 2010)
- USA SEC - PIA guide (January 2007)
- USA NIST - An Introduction to Privacy Engineering and Risk Management in Federal Systems (January 2017)
- Ireland HIQA - Guidance on Privacy Impact Assessment in Health and Social Care (December 2010)ISO/IEC 29134:2017
- ISACA GDPR Data Protection Impact Assessments (2017)
- NL NOREA – De beroepsorganisatie van IT-auditors (November 2015)
- Forum Privatheit: White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz, dritte, überarbeitete Auflage, partly based on Standard Data Protection Model
-

4.3. Research reports and academic literature

- Bieker F., Friedewald M., Hansen M., Obersteller H., Rost M. (2016): A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in: K. Rannenberg, D. Ikonomou (eds.): Privacy Technologies and Policy. Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London
- Bieker F., Hansen M., Friedewald M. (2016): Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2016, issue 4, p. 188
- Hansen M. (2016): Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge?, DuD 9/2016, S. 587
- Ireland HIQA (2010): International Review of Privacy Impact Assessments
- PIAF project consortium (de Hert, Paul et al.) deliverables: Review and analysis of existing PIA (2011), survey of DPAs on PIAs (2012), Final report with recommendations for a EU PIA framework (2012), project homepage
- Wright D., Finn R., Rodrigues R. (2013): A Comparative Analysis of Privacy Impact Assessment in Six Countries, Journal of Contemporary European Research (JCER), 9 (1), p. 160

5. Glossary

This glossary explains a number of data protection terms used in the toolkit.

Accountability	Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.
Adequacy decision	The European Commission may decide that a third country provides an adequate level of data protection. Transfers to adequate third countries do not require additional safeguards compared to transfers to recipients inside the EU.
Adequate safeguards	Measures for adducing an adequate level of protection when transferring personal data to third countries or international organisations, e.g. standard contractual clauses
Availability	Property of being accessible and usable upon demand by an authorized entity
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them
Control	In ISRM terminology, a measure that is modifying risk.
Controller	The Union institution, body, office or agency or the Directorate-

	General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law (Article 3(2)(b) new Regulation).
(personal) Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
(personal) Data breach notification	Mandatory notification of (personal) data breaches to the data protection authority
Data Protection Authority (DPA)	Public authority charged for supervising the processing of personal data. The EDPS is the DPA for the EUIs.
Data Protection Coordinator (DPC)	Some larger EUIs have DPCs as local contact points in each Directorate-General or other similar organisational division. DPCs assist the DPO.
Data Protection Impact Assessment (DPIA)	A structured process to manage the data protection risks of certain risky processing operations (Article 39 new Regulation).
Data Protection Officer (DPO)	The DPO informs and advises the controller/EUI, EUI staff and data subjects on data protection issues and ensures, in an independent manner, the internal application of data protection rules in their EUI. DPOs are also the main contact point between EUIs and the EDPS Every EUI has a DPO.
Data quality	See Article 4 new Regulation.
Data subject	Any natural person whose personal data you process, whether employed by your EUI or not.
European Data Protection Board (EDPB)	The forum in which national DPAs, the EDPS and the European Commission cooperate to ensure consistent application of data protection rules throughout the EU. Replaces the WP29.
European Data Protection Supervisor (EDPS)	The Data Protection Authority for the EUIs (see the new Regulation).
European Institutions and Bodies (EUIs)	Shorthand for all European Instituions, Bodies, Offices, Agencies and other entities under the scope of the new Regulation.
General Data Protection Regulation (GDPR)	Regulation (EU) No 2016/0679. The GDPR lays down the data protection rules applicable to private sector controllers and most public sector controllers (except for law-enforcement tasks) in the EU Member States.
Lawfulness of processing	In order to lawfully process personal data, the processing has to fall under one of the situations listed in Article 5 of the new Regulation, such as this being necessary for the performance of a task in the

	public interest assigned to a EUI by EU law.
Information Security Risk Management (ISRM)	The risk management process for ensuring that the confidentiality, integrity and availability of an organisation's assets match the organisation's objectives.
Integrity	Property of accuracy and completeness
New Regulation	Commission proposal 2017(0008), once adopted by the EU legislator. As of writing, this proposal is in the last stages of the legislative process and mostly stable.
Old Regulation	Regulation (EC) No. 45/2001.
Person responsible on behalf of the controller	While your EUI as such is the controller and remains accountable for its processing operations, responsibility is usually assumed at a lower level, e.g. by business owners of a specific processing operation.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1) GDPR). Data subjects may be identifiable directly (e.g. names) or indirectly (e.g. "a female Maltese Director-General in your EUI")
Prior check notification	Notification to the EDPS under Article 27 of Regulation (EC) No 45/2001
Privacy by default	The principle that the default settings of product and services should be privacy-protective (Article 27(2) of the new Regulation).
Privacy by design	The principle that controllers have to consider data protection both during the development and deployment (Article 27(1) of the new Regulation).
Privacy statement	An information notice informing data subjects about how a controller processes their personal data (Article 14 to 16 new Regulation).
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR)
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Example: company organising an assessment centre for your EUI, based on an

	outsourcing contract
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) GDPR).
Record	Documentation of your processing operations (Article 31 new Regulation).
Restriction of processing	The marking of stored personal data with the aim of limiting their processing in the future (Article 4(3) GDPR).
Right of information	Data subjects have the right to be informed about your processing of their personal data. Inform them by providing a data protection notice / privacy statement.
Right of access	Data subjects have the right to access their personal data held by a controller; some exemptions may apply (Article 17 new Regulation)
Right of rectification	Data subjects have the right to rectify their personal data held by a controller when they are incorrect (Article 18 new Regulation).
Right of erasure / right to be forgotten	Data subjects have the right to obtain erasure of their personal data held by a controller in some situations, such as when data are held unlawfully (Article 19 new Regulation).
Residual risk	Risk remaining after risk treatment
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. Risks have an impact and a likelihood. Can also be defined as the effect of uncertainty on objectives.
Risk treatment	Applying a control to a risk.
Risk management	The process for identifying, assessing, and controlling/treating risks.
Special categories of data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation (Article 10 new Regulation); data concerning criminal convictions and offences (Article 11 new Regulation).
Third country	Non-EU or EEA countries; transfers of personal data to third countries may require additional safeguards.
Threshold assessment	Assessment carried out by the controller, with the DPO's assistance, to find out whether a DPIA is needed.