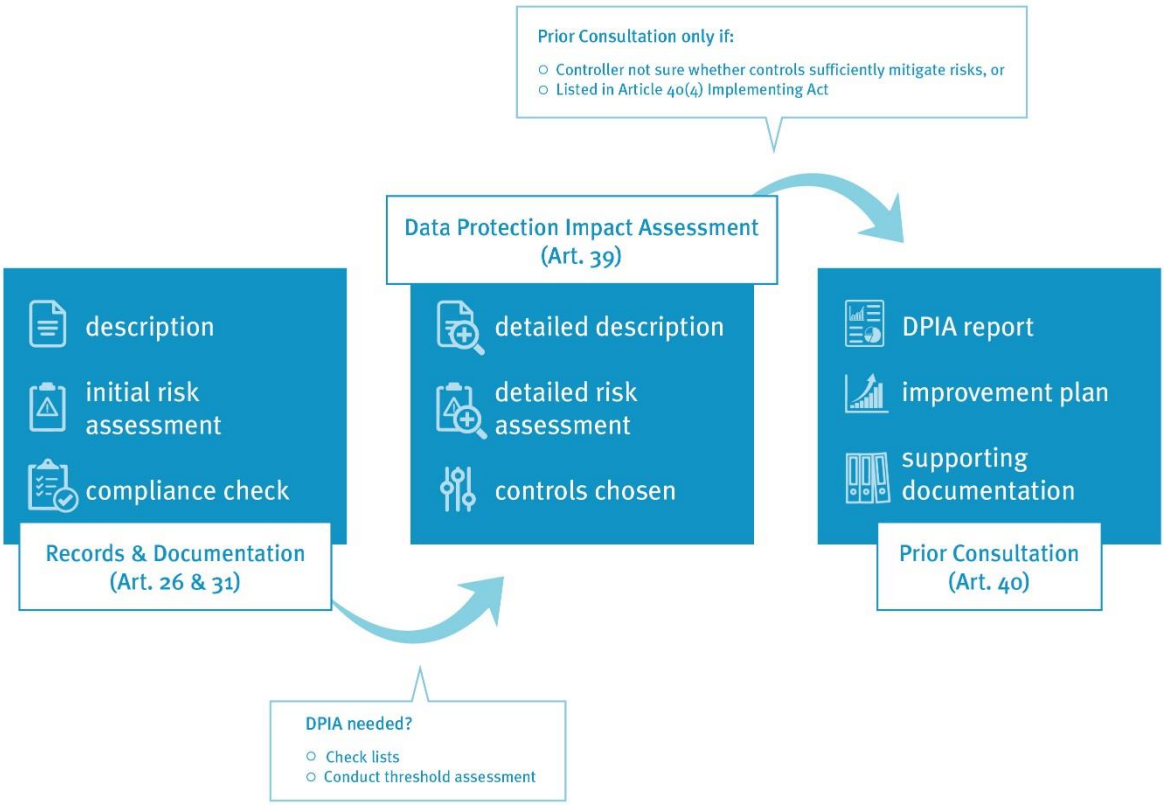
EUROPEAN DATA PROTECTION SUPERVISOR

Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies
Summary

February 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
initial risk assessment
compliance check
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

1 Accountability on the ground

When processing information about people ('personal data'), we in the EU institutions, bodies and agencies (EUIs) have to comply with certain rules to protect the privacy of those whose data we process. This is true whether this is about our own staff, beneficiaries, contractors or any other person. An update to these rules is currently in the last stages of the legislative process.[1]

In a nutshell, those rules tell you to:

(1) have a good reason for processing people's data;
(2) tell them about it;
(3) be accountable for both *what* you do and *why* you do it.

The main player are you in the EUIs who are accountable for the processing of personal data ('controllers'). You are accountable for what you do and why you do it the way you do it. This implies being compliant but also being able to *demonstrate* it.

The best way to do that is to follow a structured approach to designing and documenting processing operations. This also means that you have to think about this already when you design new processes ('privacy by design'). The European Data Protection Supervisor (EDPS) toolkit *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies* provides such guidance, summarised in this brochure.

As the new rules are not adopted yet, some provisions may change for the final version. The EDPS will update this toolkit once the legislative process will be finished. When addressing provisions that are still likely to change in the legislative process, the toolkit points that out. References to Articles refer to the Commission proposal COM(2017)0008, unless indicated otherwise.

The new rules for the EUIs build on earlier rules enacted in 2001 (Regulation (EC) No. 45/2001[2] - 'the old Regulation') and mirror those for organisations processing personal data ('controllers') in the Member States – be they public administrations, businesses, charitable associations or other organisations. Compared to the previous rules, the Regulation aligns your documentation obligations more closely to the risks caused by processing personal data. This means for example that the documentation requirements for your EUI's newsletter subscription will be lower than for a system using 'intelligent CCTV' covering publicly accessible space. These rules also take into account the status of data protection as a fundamental right under Article 8 of the Charter.

The EUIs have to lead by example on fundamental rights, including data protection. The EDPS, the supervisory authority checking how EUIs process personal data, provides extensive guidance on many aspects of compliance with these rules.

This toolkit addresses the specific situation of EUIs under the EDPS' supervision, but it is in line with the principles of the General Data Protection Regulation (EU) 2016/679 (GDPR)[3] and the guidance given by the Article 29 Working Party (WP29).[4] We will update it to stay consistent with the WP29 interpretation of the GDPR where necessary. It may thus also be of

[1] European Commission proposal: COM(2017)0008; European Parliament procedure reference: 2017/0002(COD)
[2] OJ L 8/1, 12/01/2001
[3] OJ L 119/1, 04/05/2016
[4] E.g. 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, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

interest for controllers, data protection officers (DPOs) and other interested parties outside the EUIs. As the rules for the EUIs will be largely similar to those in the GDPR, they should be interpreted the same way as well. For this reason, we occasionally refer to the GDPR as well.

If you want to know more, talk to your EUI's DPO and have a look at the toolkit – whenever you see square brackets in this brochure, the references in there tell you where in the toolkit to find more information. For further guidance on other topics, such as when and how to inform people that you're processing their data or on data protection aspects of specific business processes (recruitment, staff evaluation, administrative inquiries and disciplinary proceedings, etc.) please check the EDPS website.[5]

2 Target audience, scope, and relationship to other documents

The target audience of this toolkit are controllers and staff responsible on their behalf, DPOs, data protection coordinators (DPCs)[6], and everyone else involved in the development and management of personal data processing activities in the EUIs. 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'.[7]

In this toolkit, 'you' refers to the 'person responsible on behalf of the controller' or 'controller in practice' (business owner) of an existing processing operation or the project owner for activities in development.

This toolkit provides guidance on how to comply with the new Regulation concerning the necessary data protection documentation and risk assessments for 'risky' processing operations. It covers the following aspects and provides templates for most of them:

- how to document your processing activities;
- when to do data protection impact assessments (DPIAs);
- how to do DPIAs;
- when to send DPIAs to the EDPS for prior consultation;
- who does what in the above processes;
- transition rules from the old data protection regulation for EU institutions.

This toolkit does *not* cover:

- the high-level approach to accountability (umbrella paper);
- the role of DPOs in general;
- how, in detail, to deal with specific processing operations, such as transfers of personal data outside the EU or specific processes, such as staff selection & recruitment.[8]

[5] https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en
[6] Some of the larger EUIs have DPCs as local contact points in each Directorate-General (or similar).
[7] Article 3(2)((b) of the Regulation.
[8] For these specific situations and many more (administrative inquiries, disciplinary proceedings, leave management and flexitime, medical data etc.), the EDPS has developed more detailed guidance, please see here: https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en. The EDPS will update those documents to adapt them to the new rules.

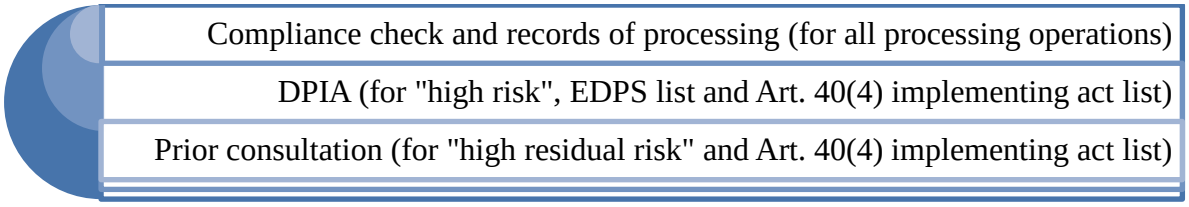
This toolkit gives you guidance on thinking about managing privacy risks for a business process in your organisation and how to document this. For specific suggested controls to implement e.g. in selection procedures, please refer to the guidelines per processing operation.

3 The accountability process

Accountability means that the controller is in charge of ensuring compliance and being able to demonstrate that compliance. In practice, top management is accountable for compliance with the rules, but responsibility is usually assumed at a lower level (business owner). The business owner / person responsible on behalf of the controller[9] for a process will be the main driver, assisted by the DPO and DPCs (Part I - Section 2, Part II - Section 2).

For most processing operations in your organisation, keeping records and doing a compliance check will be enough. Only some processing operations will require a DPIA. Out of these, only some will also require prior consultation.

Demonstrating your compliance means documenting how you process personal data and why you chose to do it the way you do it. Your documentation obligations depend on the risks posed by the nature of the processing of personal data – a newsletter subscription service will require far less documentation than a database profiling travellers for risk screening purposes. How you design a process also affects this – staff appraisal based on a simple evaluation interview with the reporting officer will require less documentation than a system automatically generating comparative metrics from a case management system and using these as input for the staff appraisal procedure.

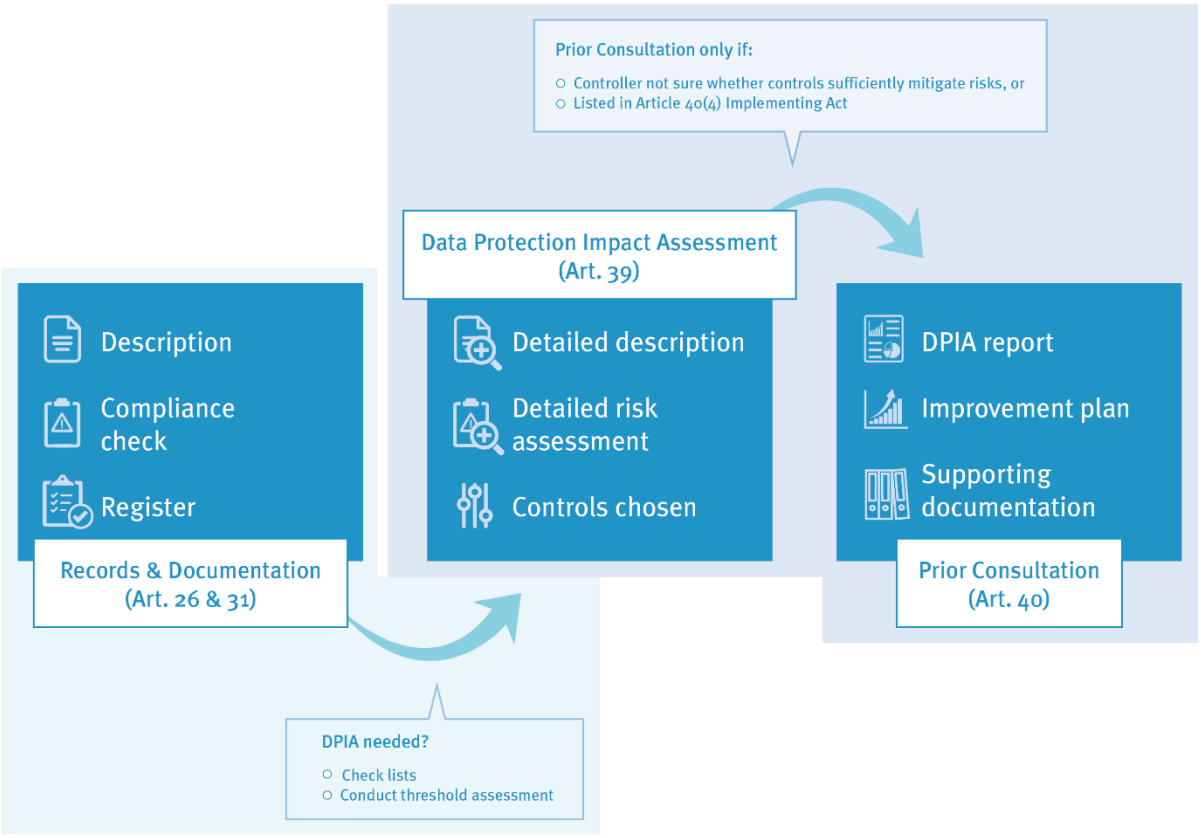


Depending on the process at hand, you may not have to go through all the steps below:

- Generate basic documentation (called ‘records’) for all processes; use this opportunity to also do a compliance check;
- check if the process is likely to result in high risks to the people whose data you process and consult your DPO if it appears to do so;
- If you need to do a DPIA, you analyse those risks in more detail and develop specific safeguards/controls to manage them;
- If the results of the DPIA still indicate high residual data protection risks, you have to consult the EDPS.

The first two steps are covered in Part I of the toolkit, the last two in Part II.

[9] 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.



4 What are records? [Part I - Section 3]

You have to keep some basic documentation for all your processing operations, called records. The **Regulation gives you a list of items** to include in the records [Part I - Section 3.1]. When you create a record, you should also **check whether your processing is compliant** with the rules [Part I - Section 3.2]. See [Part I - Annex 1] for a template you may use for this. For creating these records, you can base yourself on the already existing notifications in your EUI [Part I - Section 5]. Once you have created these records, make sure you keep them up-to-date [Part I - Section 3.3].

These records feed into a **central register** kept by your EUI and managed by the DPO [Part I - Section 3.4]. The DPO is best-placed to be the guardian of this register, but you as business owner remain responsible for the content of the records you generated. This **register should be public** [Part I - Section 3.5].

This is the data protection documentation required for most processing operations.

5 When to carry out a Data Protection Impact Assessment? [Part I - Section 4]

However, some **'risky' processing operations require further attention**. This covers **for example** processing large amounts of **sensitive personal data**, such as health data, data relating to disciplinary matters or using **profiling** techniques just to give a few examples. There are three questions that you should ask to yourself in order to know if your have to do a DPIA.

- Is the processing listed in an implementing Act under Article 40(4) of the Regulation?
- Is it listed on the list issued by the EDPS under Article 39(4) of the Regulation?
- Does the threshold assessment confirm the need for a DPIA?

If the answer to any of these three question is 'yes', you should do a DPIA. The EDPS provides a **template** you may use for this threshold assessment [Part I - Annex 6] and an **indicative list** of 'risky' processing operations in preparation for the formal list to be established under Article 39(4) [Part II - Annex 5].

6 How to carry out Data Protection Impact Assessments? [Part II - Section 3]

Under the Regulation, you have to conduct DPIAs for processing operations likely to cause 'high risks' to the people whose data you process.

The EDPS does **not impose a specific methodology** for doing so, but **provides templates** you may use for doing DPIAs [Part II - Annex 3]. If you do not want to use these templates, you can use any methodology that complies with the requirements of the Regulation [see a non-exhaustive list in Part II - Annex 4.1].

In a DPIA, you analyse your planned processing operations in more detail to see where the privacy risks are and how you can mitigate them. **This is more than information security risk management**. Once you have done this for the first time, you will have a DPIA report explaining your processing operation, the risks identified and the controls (to be) implemented. **DPIAs are an ongoing process**, not a one-time exercise– review them when your processing operations change significantly and in any case in regular intervals to keep them up to date [Part II - Section 3.8].

It is a good practice to publish your DPIA reports, at least in summary form. Publication allows displaying the work that has gone into making processing operations compliant and can foster trust with your stakeholders and the public at large [Part II - Section 3.9].

7 When to do a prior consultation [Part II - Section 4]

In a DPIA report, you have in the end three possible outcomes:

(1) You are confident that the controls chosen following the DPIA are sufficient to reduce risks to an acceptable level. In this case, implement them and go on with the project;
(2) You conclude that the controls analysed cannot reduce the risks to an acceptable level. If this happens, you should abandon the project or re-design it, as it has proven impossible to implement in a compliant way;
(3) You are not sure whether the controls you analysed and chose are sufficient for reducing the risks to an acceptable level.

In this third case, you then have to proceed to 'prior consultation' of the EDPS (Article 40 of the Regulation). The European Commission may also adopt implementing acts listing kinds of processing operations that always require prior consultation.

You will need to provide your DPIA and some other information to the EDPS [Part II - Section 4]. The **EDPS will reply within 8 weeks**; for extremely complicated cases, we can extend that deadline by another 4 weeks. In case we need further information from you, such requests suspend this deadline. In the reply, the EDPS will provide **recommendations for improving compliance** where appropriate.

8 How to get ready? [Part I - Section 5; Part II - Section 5]

Your EUI already has a certain amount of data protection documentation, so there is **no need to start from zero**. For generating records, you can **start from the notifications you sent to**

your DPO under the old Regulation (EC) No 45/2001 [Part I - Section 5]. If your notifications are up-to-date, then converting them into records should not be a lot of work. Concerning the more risky processing operations requiring DPIAs, many of them will have been subject to 'prior checking' under the old Regulation [Part II - Section 5].

There are also **other changes** coming your way with the new Regulation. For example, you will have to keep a closer eye on your **subcontractors** and will most likely need to update your **privacy statements**.[10]

9 What can your DPO do for you?

In every EUI, there is at least one Data Protection Officer (DPO), acting as a **reference point for all matters related to data protection**. In some larger EUIs, you also have Data Protection Coordinators/Contacts (DPCs) per Directorate-General. They can provide you with input on how to generate records and carry out DPIAs. If you have any questions on data protection, please contact them. However, always remember that compliance is the controller's obligation.

DPOs also act as the **main contact point between the EUIs and the EDPS** – whenever you want to ask the EDPS something, please channel this through your DPO. In many cases, they will already know the answer.

10 What can the EDPS do for you?

The **EDPS is the supervisory authority for the processing of personal data by the EUIs**. As such, we monitor and check compliance with the data protection rules - whether in response to complaints, in inspections, in reply to consultations sent by EUIs, or on our own initiative. We provide guidelines on how to be compliant, based on our experience, as well as training to help you become a leader on data protection and implement best practices.

Apart from this supervisory role, the EDPS also acts as **an advisor to the EU legislator** on new rules dealing with the processing of personal data, such as proposals for legal acts establishing new EU databases. We will also provide the **secretariat for the European Data Protection Board**, the forum in which the Data Protection Authorities of the EU Member States cooperate on cross-border issues and cooperate with data protection authorities in the EU and beyond.

[10] EDPS Guidance on Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations, available at: https://edps.europa.eu/data-protection/our-work/publications/other-documents/articles-14-16-new-regulation-452001_en.