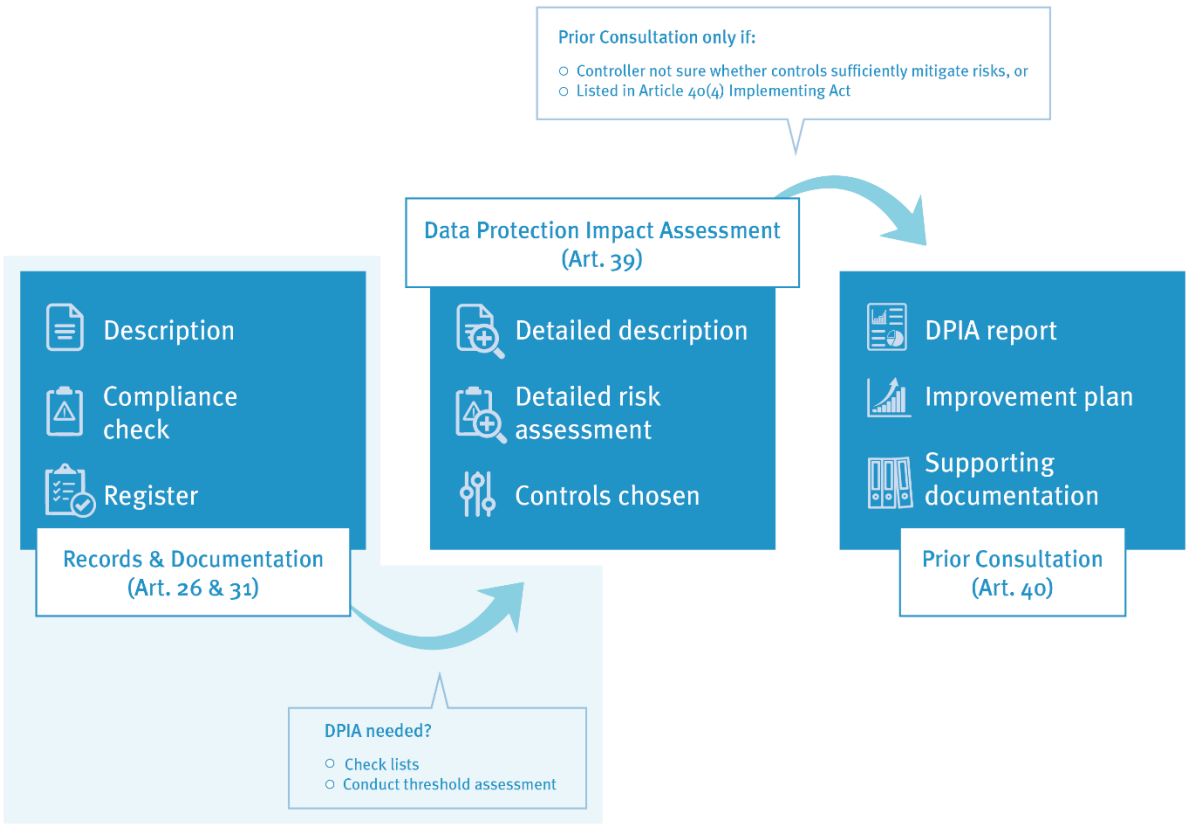
EUROPEAN DATA PROTECTION SUPERVISOR

# Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments


v1.2 December 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


**1. Introduction and scope of Part I ..... 3**
**2. Responsibilities – who does what? ..... 4**
**3. Documenting your processing operations ..... 5**
3.1 WHAT ARE RECORDS? ..... 5
3.2 COMPLIANCE AND RISK CHECK ..... 6
3.3 REVIEWING RECORDS ..... 7
3.4 KEEPING A REGISTER OF RECORDS ..... 7
3.5 PUBLICITY OF RECORDS ..... 8
**4. When to carry out a DPIA? ..... 9**
4.1 CRITERIA FOR WHEN A DPIA IS MANDATORY ..... 9
4.2 EDPS POSITIVE / NEGATIVE LISTS ..... 10
4.3 THRESHOLD ASSESSMENT ..... 11
**5. How to get ready? ..... 11**
**6. Conclusion ..... 12**
**Annexes ..... 13**
1 WHO DOES WHAT? ..... 13
2 RECORDS AND COMPLIANCE CHECKLIST ..... 14
3 FURTHER EXPLANATIONS ON RECORDS / COMPLIANCE CHECK TEMPLATES ..... 19
4 TRANSLATION TABLE ARTICLE 25 NOTIFICATIONS UNDER THE OLD REGULATION TO RECORDS UNDER THE NEW REGULATION ..... 22
5 POSITIVE/NEGATIVE LISTS ..... 23
6 TEMPLATE FOR THRESHOLD ASSESSMENT / CRITERIA ..... 25
7 REFERENCE DOCUMENTS ..... 27
8 GLOSSARY ..... 27


## Table of figures


Figure 1: Scope of part I ..... 3
Figure 2: RACI matrix records/documentation process ..... 4

# 1. Introduction and scope of Part I

As the business owner of a process / person responsible on behalf of the controller, you have to create 'records' (Article 31 of Regulation (EU) 2018/1725 - 'the Regulation'[1]) of your EUI's personal data processing operations on a per-process basis. This means e.g. one 'record' for selection and recruitment procedures and another one for anti-harassment procedures.

Part I of the toolkit shows you how to generate these records and related documentation. It also shows how to decide whether you need to do a Data Protection Impact Assessment (DPIA).

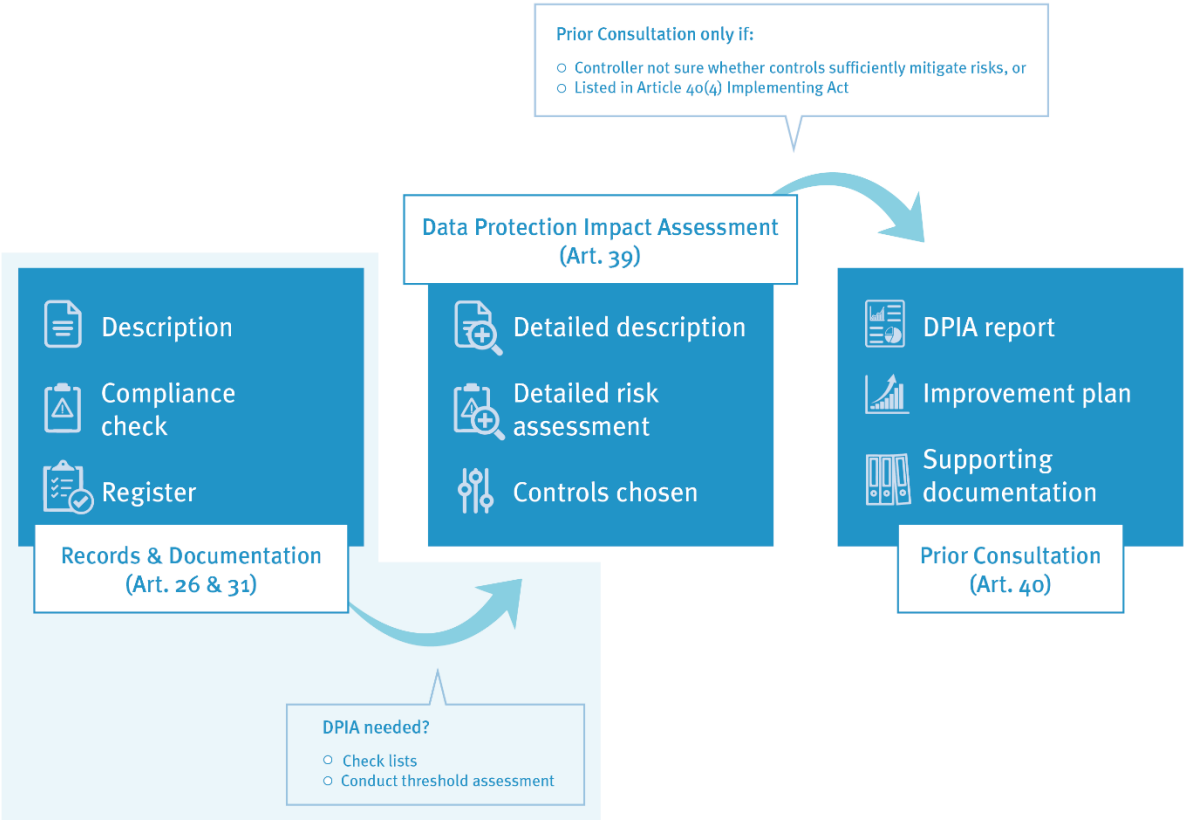



Figure 1: Scope of Part I

This part provides guidance on how to comply with the Regulation when developing new business processes ('processing activities' in data protection terminology) and how to manage the necessary data protection documentation. It covers the following aspects and provides templates for most of them:

- how to document your processing activities;
- who does what in doing so;
- how to assess whether you need to do a DPIA;
- transition rules from the old data protection regulation for EU institutions as far as records are concerned.

For the following issues, please refer to Part II instead:

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

[1] OJ L 295/39, 21/11/2018

## 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 cases 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].

It is the **controller's task to keep appropriate records** (in practice: top management accountable, business owner responsible)[4]. The EDPS strongly recommends that EUIs centralise their records in a **public register kept by the DPO**[5]. Accountability for generating records and for their content remains with the controller. While the DPO can *help* you in generating the records and supporting documentation, this is your task. Similarly, checking whether you need to do a DPIA is your job as the business owner – your DPO can help you with this, but it is your task to get it done.

The RACI[6] matrix below gives a quick overview of the different roles[7] concerning records. Please note that this a general overview – depending on the processing operations at issue, you may need to involve other teams, such as you EUI's legal unit/service.

| | Responsible | Accountable | Consulted | Informed |
|---|---|---|---|---|
| **Top Management** | | **X** | | |
| **Business owner** | **X** | | | |
| **DPO** | | | **X** | |
| **IT department** | | | **X** | |
| **Processors, where relevant** | | | **X** | |

Figure 2: RACI matrix records/documentation 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 (e.g. processors or information providers), these have to be consulted and provide their input where necessary. In most cases, your IT department will provide the technical infrastructure and will be best-placed to contribute on information security aspects.

---

[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.

[4] Articles 26 and 31 of the Regulation.

[5] See also sections 3.3 and 3.5 below.

[6] 'responsible, accountable, consulted, informed' - a framework for assigning tasks and responsibilities.

[7] 'Responsible' means having the obligation to act and take decisions to achieve required outcomes; 'accountable' means to be answerable for actions, decisions and performance; 'Consulted' means being asked to contribute and provide comments; 'informed' means being kept informed of decisions made and the process.

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 ultimately 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. Documenting your processing operations

## 3.1 What are records?

**Document your processing operations with 'records'. For legacy processing operations for which you already had Article 25 notifications under the old Regulation, you can use those as a basis for your records.**

As the person responsible on behalf of the controller, **you have to generate records for all your processing activities that involve personal data** – from your EUI's newsletters, through staff selection, to your core business tasks, to administrative inquiries and disciplinary proceedings. Records contain basic information about the processing operations such as 'Who is in charge? What are the purposes? What data do we process about which people?' They are the foundations of your data protection documentation and one of the first things the EDPS will look at when assessing your compliance with data protection rules.

Even if a new project is not yet advanced enough to start creating a record, it is **always a good idea to talk to your DPO** – the earlier you realise problematic aspects of your planned processing operations, the easier it will be to correct them.

**Records are not new**: under Article 25 of the old Regulation (EC) 45/2001, you had to submit notifications with similar content to the DPO. You may re-use those to generate your records. The information items in records are very similar to those you have to include in data protection notices / privacy statements informing people about your processing operations. You may **reuse text** from one for the other.

Article **31 of the new Regulation** gives you a list of information to be included in records:

a) names and contact details of the controller (incl. joint controllers, where applicable), the DPO and any processors (where applicable)
*Who is in charge? Who can people talk to? Use functional mailboxes, not the personal mailboxes of the business owner and DPO (better for business continuity and easier to update)*[8]*. In the end, it is the role in the organisation that matters, not the person currently occupying that role. If you use a processor/contractor to process personal data for you, mention it (e.g. outsourced IT services or pre-employment medical checks); if you are jointly responsible with another EUI or another organisation, say so (e.g. two EUIs sharing a medical service).*

[8] While Article 31 of the Regulation talks about the 'name' of the DPO here, Articles 15 and 16 (on information to data subejcts) only refer to the contact details. The EDPS is of the opinion that providing the name of the natural person currently fulfilling the DPO role in an EUI is not necessary here – what matters is that persons affected have a contact point in the organisation.

b) the purpose of the processing;
*Why are you doing this? Provide a very concise description of what you intend to achieve with the processing of personal data; if you rely on a specific legal basis, mention it as well (e.g. staff regulations for HR procedures, tasks assigned to your EUI by EU law).*

c) a description of the categories of persons affected and which data about them will be processed;

*Who is affected? What do you keep about them? In case data categories differ between different categories of persons, explain (e.g. suspects vs. witnesses in investigations).*

d) the categories of recipients to whom the data will be disclosed;

*Who will have access to this information (both in-house and outside)? Who has access to which parts of the data? Note: You do not have to mention entities that may only have access in the course of a particular investigation (e.g. OLAF, EO, EDPS)*[9].

e) transfers to recipients in third countries or international organisations, stating which third country/international organisation and documentation of the suitable safeguards for this transfer;

*In case you give data to such parties, who are they and how do you ensure that they process it fairly (e.g. processor in a third country using standard contractual clauses)?*

f) planned time limits for erasure of the different categories of data;

*For how long do you keep the information, starting from when? Indicate your administrative retention period, including its starting point; differentiate between data categories or categories of persons where needed (e.g. in selection procedures: candidates who made it onto the reserve list vs. those who did not).*

g) where possible, a general description of the security measures adopted.

*What can you disclose about how you secure the data processed? This does not mean disclosing your detailed information security measures, but giving a general description that does not prejudice the effectiveness of those measures.*

The first part of the **template form in Annex 2** contains these items, instructions for filling them out and a sample record. Only this first part, containing the **items listed in Article 31 of the new Regulation, falls under the publication requirement** discussed in section 3.5 below.

## 3.2 Compliance and risk check

**When generating your records, take this opportunity to also check that your processing operation complies with data protection rules. You have to comply with the rules and be able to demonstrate this compliance.**

Generating records is a **good moment for also checking the substantive compliance** with data protection rules, for which controllers are accountable. Controllers have to design processes in a way that ensures they are compliant with the rules (see Articles 4(2) and 26 of the Regulation).

[9] See Article 3(1)(13) of the Regulation; for further background on the equivalent rules in GDPR, please see recital 31 GDPR.

The second part of the form in Annex 2 provides a **short checklist** for the most important rules. You have to comply with the Regulation and be able to demonstrate this compliance, taking into account the risks caused by the processing operations (Article 26 and recital 38 of the Regulation). This **'risk mindset'** is one of the big changes compared to the old rules: always think about how the processing could affect those whose data you process. What does it do to them? How does it affect them? Both if things go according to plan and when things go wrong. This checklist can be a tool for doing so. While not formally speaking part of the record, it shows that you thought about the data protection implications of the processing.

There are two basic aspects here - 'is this processing lawful?' and 'do we comply with the data protection principles?' The template in Annex 2 includes explanations on how to fill it in and you can find further legal background information in Annex 3. Checking these compliance aspects at the same time as generating your records and documenting them helps you to be compliant and to demonstrate this ('accountability' in Article 4(2)).[10] For the information security aspects of data protection compliance, make sure that you have a proper information security risk management process in place and choose controls that are appropriate to the risks caused by the processing operations.[11]

At the end of the compliance check, you will also find a few screening questions to help you in finding out whether your processing operations may pose 'high risks' and thus require further analysis. If you tick any of those boxes, talk to your DPO – you may need to do a DPIA. For more information on DPIAs, please refer to Part II of this toolkit.

## 3.3 Reviewing records

**Ensure that records always reflect the reality of the processing operations they relate to.**

Your records have to reflect the reality of your EUI's processing operations. This means that you have to **ensure they are up-to-date**. When planning changes to your processing operations, check if the record needs updating. It is a **good idea to formally include this check in your change management process**. It may also be a good idea to conduct regular reviews independently of planned changes in order to catch changes that may have gone unnoticed.

## 3.4 Keeping a register of records

Your EUI has to keep these records in writing (including in electronic form - Article 31(3) of the Regulation) and make them available to the EDPS upon request (Article 31(4)). In accordance with Article 31(5), 'unless it is not appropriate taking into account the size of the institution or agency, Union institutions and bodies shall keep their records of processing activities in a central register'.

**The EDPS strongly recommends that all EUIs keep a central register of records and that the DPO keep this register.**

[10] Logically, the compliance check comes before the record: in case you realise that you cannot legally carry out certain processing operations, you should abandon the project, so that there will be no need for a record. In practice, it makes sense to put the record before the compliance check: first describing what you (plan to) do and then why you do it this way and how you ensure that it complies with the applicable rules makes for easier reading.

[11] For more details, please see EDPS guidance on security measures for personal data processing (https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en) and your EUI's Information Security Risk Management (ISRM) framework.

Under the old Regulation, EUIs kept a central register. For practical reasons, it makes a lot of sense to continue this practice:

- it allows an easy overview of your organisation's processing activities, enabling it to be in control of what it is doing;
- it makes answering to requests concerning records, whether coming from the EDPS or from other stakeholders, easier;
- it makes your records easier to compare, making quality control of your records easier;
- it helps your DPO in their task to ensure the internal application of the Regulation;
- it makes it easier for you to find out how other similar processing operations in your organisation have been documented, facilitating generating records.

The EDPS recommends that EUIs' DPOs keep these registers, for the following reasons:

- DPOs are knowledge hubs on data protection - if you have questions on how to comply with data protection rules, they are the first person to talk to; having all records on hand will allow the DPO to better reply to any questions you may have;
- this enables DPOs to have an overview of organisations' processing activities, helping them to provide better advice (e.g. on how other parts of the organisation deal with similar issues);
- the Article 25 register under the old Regulation 45/2001, which was the functional equivalent of the register under Article 31(5) of the Regulation, was kept by the DPO. Continuing this practice reduces the need for organisational changes.

You must, however, be aware **that even if it is the DPO *keeps* the register of records, the EUI as controller (and by extension, you as person responsible on behalf of the controller) remains responsible for the *content* of the records**.

Under the old rules, we recommended that DPOs keep an 'inventory' of planned processing operations that weren't advanced enough in their planning to have a full 'Article 25 notification' (the predecessor of records) yet. We maintain this recommendation, as such an 'inventory' can be a valuable planning tool.

## 3.5 Publicity of records

Records are an important tool for checking and documenting that your organisation is in control of its processing activities. In accordance with Article 31(5) of the Regulation, EUIs shall make their registers publicly available.

**EUIs are obliged to make Article 31 records publicly accessible, preferably through publication on the internet, continuing the practice of many EUIs for Article 25 notifications under the old Regulation.**

This publication has many advantages:

- it contributes to the transparency of EUIs[12];
- It helps strengthen public trust;
- it makes knowledge-sharing between EUIs easier.

[12] See also Article 15(1) TFEU.

**Please note that this publication requirements only applies to the Article 31 records strictly speaking (i.e. those items listed in Article 31(1) of the new Regulation) and not to other documentation your EUI may hold**. The template in Annex 2 is split into several parts, making it easy to only publish the information that Article 31 obliges you to publish.

# 4. When to carry out a DPIA?

## 4.1 Criteria for when a DPIA is mandatory

You will not have to do DPIAs for all processing operations. Only those that are likely to pose a 'high risk to the rights and freedom of data subjects' require a DPIA. As the person responsible on behalf of the controller, preparing the DPIA is your task, assisted and guided by your EUI's DPO.

**You have to carry out a DPIA when your process meets at least one of the criteria below:**

**(1) it is on the list of kinds of risky processing operations to be issued by the EDPS;**
**(2) it is likely to result in high risks according to your threshold assessment.**

The new Regulation makes provision for several non-exhaustive lists of processing operations that require DPIAs and for an assessment by you for those cases that are not on these lists. To find out whether your planned processing operations require a DPIA, ask yourself these questions:

1. Is it listed on an EDPS list issued under Article 39(4)? If so, conduct a DPIA;
2. If it's not on either of the lists, conduct a threshold assessment to find out whether you have to do a DPIA.

According to Article 39 of the Regulation (emphasis added):

> '*(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*
>
> […]
>
> *(3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
>
> > *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; .*
> >
> > *(b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or .*
> >
> > *(c) a systematic monitoring of a publicly accessible area on a large scale.'*

This list is **non-exhaustive**, as indicated by the use of 'in particular'. There may be other processing operations clearing the threshold of 'high risk to the rights and freedoms of natural

persons'. For DPIAs under the GDPR, the WP29 has provided guidance, since endorsed by the EDPB, including criteria for processing operations subject to DPIAs under the GDPR.[13] **The threshold assessment helps you in assessing whether your planned processing operations meet this threshold.**

In accordance with paragraph 4 of the same Article, the **EDPS shall establish and make public a list of 'kinds of processing operations' subject to a DPIA**. The EDPS may also establish a negative list of kinds of processing operations not subject to DPIAs, in accordance with paragraph 5 of the same Article.

Under Article 40(4) of the Regulation, the European Commission may adopt implementing acts listing kinds of processing operations that require prior consultation. In order for the EDPS to be able to reply to those consultations, you should do a DPIA before. Should the European Commission issue such implementing acts, **we will add the listed processing operations to our list to be issued under Article 39(4)**. That way, you will only have one list to check.

If you conclude that a DPIA is necessary, please refer to part II of the *accountability toolkit*.

Article 39(9) of the Regulation creates an **exemption** from the requirement to conduct DPIAs. This Article states that for processing operations with (1) a specific legal basis regulating the specific processing operation or set of operations in question, and for which (2) a DPIA was already carried out as part of a general impact assessment for the proposed legal basis, no DPIA is needed. In order to qualify as a DPIA under the Regulation, such assessments would need to be substantially more detailed than the impact assessments currently seen for legislative proposals. Put simply, current impact assessments in the EU legislative process seek to answer the question 'is this proposal a good idea?'[14], while DPIAs in the EUIs seek to answer the question 'how can we fulfil this task attributed to us in a compliant and privacy-friendly way?'.

Additionally, even where a DPIA according to the standards of the Regulation was carried out at the stage of the proposal for the legal basis, it would very likely require a review before entry into operations. The reason is that the adopted legal basis may differ from the proposal in ways that affect the impact on privacy and data protection. Additionally, it is usually not the case that all design choices with an impact on privacy and data protection are already determined by the legal basis. **In practice, such DPIAs in the legislative process can *at most* be the first iteration of the DPIA process.**

## 4.2 EDPS positive / negative lists

**If the kind of processing operation you want to implement is included on the EDPS' positive list under Article 39(4) of the Regulation, do a DPIA.**

Please see Annex 5 for a list of some common processing operations in the EUIs, together with an indication of whether or not they require a DPIA. This list is non-exhaustive. This list is not yet *the* list of processing operations (not) requiring a DPIA, but aims at providing some guidance in the interim period. **As soon as we adopt the formal Article 39(4) list, we will update this guidance.**

In accordance with Article 40(4) of the new Regulation, the European Commission may adopt implementing acts requiring prior consultation for specific cases of processing operations for

[13] See http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[14] For help in answering this question as far as is concerns data protection aspects please see EDPS' necessity toolkit.

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. These implementing acts will apply to all EU institutions, not just to the European Commission itself.

In order for the EDPS to be able to reply to such prior consultations (see also part II - section 4), you should do a DPIA before. So far, the European Commission has not adopted such implementing acts. **Should the European Commission do so, we will also include those kinds of processing operations on our Article 39(4) list**.

### 4.3 Threshold assessment

**For processing operations that do not figure on the list for mandatory DPIAs, but which you and/or your EUI's DPO still suspect may be high risk, conduct a threshold assessment using the template in Annex 6. In general, if you tick two or more of the criteria, you should do a DPIA. Document this threshold assessment.**

In case your planned processing operations do not figure on either list and you are not sure if a DPIA is required, consult your DPO and carry out a threshold assessment. **Annex 6 provides a template** for conducting this threshold assessment.

This template is **based on the criteria for 'kinds of risky processing operation' issued by the WP29[15] and endorsed by the EDPB**, with some adaptations for the specific context of the EUIs. For example, the Staff Regulations already explain how staff appraisal works in the EUI, reducing both controller's leeway in how to organise it and staff's vulnerability (as e.g. recourse mechanisms are already legally defined).

The template asks whether the processing at hand shows certain characteristics – e.g. a purpose to exclude persons from a right, benefit or contract, or including the processing of special categories of data, such as health data. If so, explain how and why exactly; in borderline cases, you should also describe why you do not consider the criterion met. The criteria go beyond the indicative list in Article 39(3), based on the WP29's interpretation of equivalent rules in the GDPR. **In general, if you tick two or more of the criteria, you should do a DPIA**.

However, the assessment cannot be reduced to a simple calculation of the number of criteria met. This is not an automated decision. Indeed, in some cases, a processing meeting only one of these criteria may require a DPIA. In other cases, a DPIA may not be necessary despite meeting two or more criteria. **If you tick two or more criteria and do not consider that the processing would in fact cause high risks for the persons affected, explain why after consulting your EUI's DPO**.

## 5. How to get ready?

Keeping track of your processing operations is not a new obligation. Under Article 25 of the old Regulation, you, as the person responsible on behalf of the controller, had to notify your DPO of all processing operations involving personal data. Your DPO kept these in a publicly accessible register.

[15] See footnote 13 above.

**Start from your existing notifications under Article 25 of the old Regulation for generating records. Generate records for new processing operations when developing them.**

These notifications can serve as a basis for generating records (see Annex 4 for a correspondence table). For existing processing operations, transform your existing Article 25 notifications into records. If your notifications are up-to-date, then converting them into records should not be a lot of work. For new processing operations, generate records when developing them.

The **Regulation does not include a transition period apart from the usual 20 days following publication in the Official Journal of the EU.** Transform your Article 25 notifications into records as soon as possible.

If you have to prioritise, start with the Article 31 records for your riskier processing operations. The compliance check is a tool to help you be able to provide evidence on why you chose to do process the data the way you do.

# 6. Conclusion

Part I of the *accountability toolkit* provided you with practical guidance on how to generate records of your processing operations and to find out whether you need to do a DPIA. For many processing operations, you will only need the record.

As the person responsible on behalf of the controller / 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.

**Records are the foundation of your data protection documentation**. Failure to keep records may result in an administrative fine against your EUI.[16] 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 records. Similarly, when there's a data breach in your EUI and you have to notify the EDPS[17], we will ask for the relevant record(s).

You will not have to create records from zero, but can start from the notifications you already did under the old Regulation. Make an effort to update these quickly, as records are the basis of your data protection documentation.

Records are not an end in themselves, but are a tool to show that you have thought about data protection compliance when designing your processing operations.

**Some riskier processing operations require additional analysis**. If you conclude that your processing operations require a DPIA, go on to the DPIA. Depending on the outcome of the DPIA, you may also have to do a 'prior consultation' to the EDPS. For further guidance on all those parts, please refer to Part II of the toolkit.

[16] Article 66 of the Regulation; a draft guidance paper has been sent to DPOs for information.

[17] Article 37 of the Regulation; EDPS Guidelines on notifying data breaches are available here: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-personal-data-breach-notification_en .

# 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 records;
- answer compliance check questions;
- conduct check whether you need to do a DPIA.

DPO:

- provide feedback on draft records and other draft documentation;
- keep register of records;
- reply to consultations from controllers / business owners;
- provide liaison point between EUI and EDPS.

Other functions (such as IT or legal)

- support controller/business owner and DPO as needed.

## 2 Records and compliance checklist

Under Article 31 of the new Regulation, EUIs have to keep records of their processing operations. This template covers two aspects:

1. mandatory records under Article 31 of the new rules (recommendation: publicly available)
2. compliance check and risk screening (internal).

The header and part 1 should be publicly available; part 2 is internal to the EUI. By way of example, column 3 contains a hypothetical record on badges and physical access control in a EUI.

| Nr. | Item | Explanation | Example: access control |
|---|---|---|---|
| | **Header - versioning and reference numbers (recommendation: publicly available)** | | |
| 1. | Last update of this record | | 25/05/2018 |
| 2. | Reference number | For tracking; if your EUI keeps a central register, contact the keeper of that register for obtaining a reference number. | EUI/Logistics/1.1 |
| | **Part 1 - Article 31 Record (specific legal obligation to publish – see Article 31(5))** | | |
| 3. | Name and contact details of controller | Use functional mailboxes, not personal ones, as far as possible - this saves time when updating records and contributes to business continuity. | Controller: EUI, Europe Square 1, Town, Member State<br>Contact: Director Logistics, EUI<br>fmb-logistics@eui.europa.eu |
| 4. | Name and contact details of DPO | This field will be pre-filled. | DPO, EUI<br>dpo@eui.europa.eu |
| 5. | Name and contact details of joint controller (where applicable) | If you are jointly responsible with another EUI or another organisation, please indicate so here (e.g. two EUIs with shared medical service). If this is the case, make sure to mention in the description who is in charge of what and who people can address for their queries. | Not applicable |
| 6. | Name and contact details of processor (where applicable) | If you use a processor (contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks). | Not applicable |

| Nr. | Item | Explanation | Example: access control |
|---|---|---|---|
| 7. | Purpose of the processing | Very concise description of what you intend to achieve; if you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures). | To ensure physical security on EUI premises by controlling access both to EUI premises in general and to sensitive areas inside EUI premises (e.g. archive rooms); to keep track of how many people are in the building for evacuation purposes, both in line with EUI's security decision, Articles X and Y. |
| 8. | Description of categories of persons whose data [EUI] processes and list of data categories | In case data categories differ between different categories of persons, please explain as well (e.g.: suspects vs. witnesses in administrative inquiries) | We process the following data on every person to whom an access badge for EUI premises has been issued (i.e. staff & on-site contractors, excluding accompanied visitors):<br>• name & photo [printed on badge and kept centrally];<br>• link to EUI [staff/contractor, kept centrally];<br>• badge number [only item stored in RFID tag in badge];<br>• doors/gates the badge is valid for [kept centrally];<br>• end of badge validity [printed on badge and kept centrally];<br>• when badge is swiped at doors/gates: timestamp, ID of gate/door, badge number [kept centrally]. |
| 9. | Time limit for keeping the data | Indicate your administrative retention period including its starting point; differentiate between categories of persons or data where needed (e.g. in selection procedures: candidates who made it onto the reserve list vs. those who did not). | We keep the data for 2 months from expiry/revocation of the badge, except for the access logs, which we keep for 2 months on a rolling basis. |
| 10. | Recipients of the data | Who will have access to the data within your EUI? Who outside your EUI will have access?<br>Note: no need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS). | EUI Security officer for following up on security incidents and investigations.<br>Guards only have access to number of people currently in the building (aggregate, no personal data). |
| 11. | Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards? | E.g. processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards. | No |
| 12. | General description of security measures, where possible. | Include a general description of your security measures that you could also provide to the public. | We keep data on badge holders and access logs electronically in systems with limited access and secured by standard EUI security practices in line with our ISO 27001-certified |

| Nr. | Item | Explanation | Example: access control |
|---|---|---|---|
| | | | information security management system. The only information stored electronically (RFID tag) on the badge is the badge number. It cannot be read from more than 5 cm away. |
| 13. | For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement: | While publishing the privacy statement is not strictly speaking part of the record, doing so increases transparency and adds no administrative burden, since it already exists. | [link to privacy statement] |
| | **Part 2 - compliance check and risk screening (internal)** | | |
| | **Compliance check (Articles 4 and 5)** | | |
| 14. | Legal basis and necessity for processing (see Article 5 of the new Regulation):<br>(a) necessary for performance of tasks in the public interest assigned by Union legislation<br>(a2) (a) as per recital 17, second sentence<br>(b) necessary for compliance with legal obligation incumbent on controller<br>(c) necessary for performance of a contract to which the DS is party<br>(d) consent<br>(e) vital interest | Tick (at least) one and explain why the processing is necessary for it. Examples:<br>(a) a task attributed to your EUI by legislation, e.g. procedures under the staff regulations or tasks assigned by an Agency's founding regulation. Please mention the specific legal basis (e.g. "Staff Regulations Article X, as implemented by EUI IR Article Y", instead of just "Staff Regulations")<br>(a2) not all processing operations required for the functioning of the EUIs are explicitly mandated by legislation; recital 17 explains that they are nonetheless covered here, e.g. internal staff directory, access control.<br>(b) a specific legal obligation to process personal data, e.g. obligation to publish declarations of interest in an EU agency's founding regulation.<br>(c) this is rarely used by the EUIs.<br>(d) if persons have given free and informed consent, e.g. a photo booth on EU open day, optional publication of photos in internal directory;<br>(e) e.g. processing of health information by first responders after an accident when the person cannot consent. | (a2) not specifically mentioned in primary or secondary EU legislation, but required for safety and security of staff, premises and information. See also EUI decision on security 2017/XXXX, Articles X and Y. |

| Nr. | Item | Explanation | Example: access control |
|---|---|---|---|
| 15. | Purpose definition | Do you list all purposes in point 7 above?<br><br>Are the purposes specified, explicit, legitimate? Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)? | Yes.<br><br>Checking that only authorised persons access EUI premises serves to ensure safety and security of our staff, information and other assets.<br><br>We also use access logs for knowing the number of persons currently present in the building (for evacuation purposes).<br><br>Logs may, on a case-by-case basis also be used for investigating incidents (e.g. "who entered the archive room during the period files disappeared?") in accordance with applicable procedures (see record EUI-123.4 on administrative inquiries), which does not appear incompatible.<br><br>We tell badge holders about this when issuing the badge (see privacy statement). |
| 16. | Data minimisation | Do you really need all data items you plan to collect? Are there any you could do without? | Photo, name and expiry date on badge are necessary for visual checks by security guards; badge number is necessary for managing access rights to restricted areas and revocations.<br><br>Keeping access logs (who, when, where) is necessary for investigating incidents such as thefts or disappearance of documents. |
| 17. | Accuracy | How do you ensure that the information you process about people is accurate? How do you rectify inaccurate information? | Name and photo are collected directly from person requesting a badge. Clocks in access gates are synchronised. Badge holders can request to have their name and photo changed. |
| 18. | Storage limitation | Explain why you chose the storage period(s) mentioned in point 9 above.<br><br>Are they limited according to the maxim "as long as necessary, as short as possible"? In case you only need some information for longer, can you split storage periods? | 2 months for access logs strike a balance between still being able to investigate incidents (which may not be detected immediately, e.g. theft over a holiday period) and not keeping logs for too long.<br><br>Information on badge holders has to be kept for the duration of badge validity. Keeping it for 2 months after expiry/revocation still allows us to investigate incidents possibly involving staff who left recently (otherwise we would not know whom an expired badge related to). |

| Nr. | Item | Explanation | Example: access control |
|---|---|---|---|
| 19. | Transparency: How do you inform people about the processing? | E.g. privacy statements on forms, e-mail notifications; if you do not want to inform people (or only inform them after the fact), consult your DPO! | Privacy statement on badge request form and short information notice on back of badge with link to published privacy statement. |
| 20. | Access and other rights of persons whose data you process | How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react? If you think there could be situations where you would want to refuse e.g. granting access, talk to your DPO. | See privacy statement: e-mail to logistics@eui.europa.eu; we will reply as per standard deadlines and procedures in EUI's data protection implementing rules (EUI Decision 2018/1234, section Y). |
| | **High risk identification** | | |
| 21. | Does this process involve any of the following?<br>• data relating to health, (suspected) criminal offences or otherwise considered sensitive ('special data categories');<br>• evaluation, automated decision-making or profiling;<br>• monitoring data subjects;<br>• new technologies that may be considered intrusive. | Some risky processing operations require additional safeguards and documentation. If you ticked any of these items, talk to your DPO for more information and guidance. | No |
| | **Part 3 - Linked documentation (internal)** | | |
| 22. | (where applicable) links to threshold assessment and DPIA | If you have carried out a threshold assessment and/or DPIA, refer to them here | n/a |
| 23. | Where are your information security measures documented? | EUI's rules on information security most likely oblige you to document your security measures; appropriate information security is also a data protection requirement. Please provide a link to relevant information security documentation. | [link to InfoSec documentation] |
| 24. | Other linked documentation | Please provide links to other documentation of this process (e.g. project documentation, handbooks) | [link to physical security concept for EUI] |

# 3 Further explanations on records / compliance check templates

The template in Annex 1 already contains some explanations on how to fill it in; in this annex, you will find further legal background information. There are two basic parts here - 'is this processing lawful?' and 'do we comply with the data protection principles?'

## Article 5 - lawfulness of processing

For the first question, the processing has to fit under one of the conditions in Article 5 of the Regulation. This is the question of 'why are we allowed to do this at all?':

*'Article 5 Lawfulness of processing*

*1. Processing shall be lawful only if and to the extent that at least one of the following applies:*

*a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;*
*b) processing is necessary for compliance with a legal obligation to which the controller is subject; .*
*c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; .*
*d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; .*
*e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.*

*2. The tasks referred to in point (a) and (b) of paragraph 1 shall be laid down in Union law.'*

In most cases, you will base yourself on **point (a).** Examples are tasks that EU legislation tells your institution to do – whether this relates to your EUI's specific tasks, or administrative rules on e.g. staff management or procurement in accordance with the Staff and Financial Regulations. These specific legal bases may also provide additional instructions on aspects of the processing (data categories, conservation periods, etc.).

According to the second sentence of recital 22 of the Regulation, point (a) also 'includes the processing of personal data necessary for the management and functioning of those institutions and bodies', e.g. keeping an internal staff directory. This is mentioned as (a2) in the form.

**Point (b)** is only for specific legal obligations to process personal data, e.g. the publication of declarations of interests specifically mandated in some EU agencies' founding regulations.[18]

**Point (c)** refers to processing that is necessary for the performance of a contract to which the person whose data you are processing is party or preliminary steps for entering into such a contract. EUIs rarely use this - an example from the private sector would be delivering goods by mail order: having the delivery address is necessary for the vendor to fulfil its part of the contract (keeping it afterwards, however, may not be).

[18] The line between points (a) and (b) is that in point (a) your EUI is given a task which requires the processing of personal data to fulfil it (e.g. staff appraisal), while in point (b), your EUI has a specific obligation to process personal data clearly spelled out in EU law with no margin of manoeuvre on how to implement it (e.g. 'the Agency shall take steps to prevent and detect conflicts of interests' vs. 'the declaration of interests of the Executive Director shall be published')

**Point (d)** refers to processing individuals have consented to. Such consent needs to be free, informed and specific.[19] EUIs do not frequently use this ground for lawfulness, as the vast majority of the personal data they process fall under point (a) above. Examples where EUIs rely on consent would be newsletters subscriptions or a photo booth on EU open day.

**Point (e)** is about processing in the vital interest of the person affected or another natural person. An example would be emergency medical care by first responders following an accident at work.

In some cases, you may rely on different points above for different aspects of the processing. For example, having an internal staff directory is 'necessary for the management and functioning' of your EUI, but having staff photos in it is not. You can offer the possibility for staff to upload photos based on their consent, but you cannot force or pressure them to do it.

## Article 4 - data protection principles

The data protection principles in Article 4 provide the basis for the more detailed rules in the new Regulation. This is the question of 'how do we do it?':

*'Article 4 - Principles relating to processing of personal data*

*1. Personal data must be:*

*a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
*b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes ('purpose limitation');*
*c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
*d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
*e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
*f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

*2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').'*

[19] See Article 29 Working Party Opinion 15/2011 on consent (WP 187).

For each of these points, ask yourself how your EUI complies with these requirements, taking into the additional explanation below:

**'Lawful'** in point (a) relates back to the check of Article 5 above.

Point (a) also refers to '**transparency'**, meaning that you must tell people that, why and how you process their personal data (as further specified by Articles 14 to 16). Some restrictions are possible, think e.g. for the early stages of an OLAF investigation. If you collect the data directly from the persons affected, e.g. via a questionnaire, provide this information at that moment. If you collect them from elsewhere, think about how you can inform people - simply publishing a data protection notice is usually not enough, as it may not necessarily reach the persons concerned. For more information, see the EDPS guidance on Articles 14 to 16 of the Regulation[20], as well as on Article 25.[21]

Part of the **'fairness'** mentioned in point (a) is also that the persons whose data you process have certain rights to intervene (as further specified in Articles 14 and 17 to 24 of the new Regulation), e.g. to know what data you keep about them, to have it corrected if necessary, to have it deleted if it is kept unlawfully etc. For more information, see the Guidelines on data subjects' rights[22]. This also means designing your systems and processes in a way that you can easily reply to such queries.

The first part of point (b) is already covered by the **'purpose'** field in the record. This principle is also linked to fairness: you have to clearly define the purposes so those affected know what to expect. This requires you to clearly articulate why your EUI is processing personal data. Strict rules on further processing aim to prevent situations like information being re-used to retaliate against whistle-blowers. 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 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.

**'Data minimisation'** in point (c) means that for each data category you must be able to explain why it is necessary for fulfilling the purpose of the processing - ask yourself 'Do we really need this for our purpose? Could we do without this data item?'[23]

**'Accuracy'** in point (d) means that you must make all reasonable efforts to ensure that the data you process are accurate, since decisions based on wrong information may have negative impacts on persons and may expose your EUI to liability. This is especially important if you do not directly collect the data from the people they are about, but from other sources. In some processing operations, the factual accuracy of statements may be in dispute between the parties affected (think 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

[20] https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf
[21] A draft guidance document on internal rules under Article 25 of the Regulation has been sent to DPOs for information.
[22] https://edps.europa.eu/data-protection/our-work/publications/guidelines/rights-individuals_en
[23] Note the difference to the necessity of the processing as a whole (when explaining Article 5(a) above: this is about 'After we've established that we should be doing this, *what do we need to do it*?'

recorded; the other party should be able to complement the information recorded and provide its own view on the matter.[24]

The principle of **'storage limitation'** in point (e) means that for all the personal data processed, you need to have a reason (linked to the purpose, see above) for keeping them as long as you do. In some cases, applicable EU legislation lays down conservation periods, but in others, it is for your EUI to determine them. In establishing periods, follow the maxim of 'as long as necessary, as short as possible' based on your business needs – conservation periods are not a technical question! If data have to be kept for purposes of proof or similar, restrict the access to them to the specific user profiles that need it.

Finally, point (f) tells you must process personal data in a way that ensures **'appropriate security'**. What is 'appropriate' depends on the risks of the processing (see also Article 26). This includes both technical and organisational measures. In many cases, you will be able to refer to your general information security risk management (ISRM) documentation here. For further guidance, see EDPS guidance on security measures for personal data procesing[25].

The EDPS has provided guidance materials on many of these aspects.[26] Where necessary, the EDPS will update them in light of the new Regulation, once adopted. For more information, contact your DPO.

## 4 Translation table Article 25 notifications under the old Regulation to records under the Regulation

Article 25 of the old Regulation listed these mandatory items for notifications to the DPO:

(a) the name and address of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;
(b) the purpose or purposes of the processing;
(c) a description of the category or categories of data subjects and of the data or categories of data relating to them;
(d) the legal basis of the processing operation for which the data are intended;
(e) the recipients or categories of recipient to whom the data might be disclosed;
(f) a general indication of the time limits for blocking and erasure of the different categories of data;
(g) proposed transfers of data to third countries or international organisations;
(h) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 to ensure security of processing.

EUIs used their own templates for these notifications, sometimes including additional items, such as specifically noting whether a processor was involved. Article 31 of the Regulation, as explained above in section 3.1, lists the mandatory items for records under the Regulation.

[24] 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.

[25] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en

[26] See https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

Matching these Articles shows the commonalities and differences. As you will see, a large part of the information required for records is already available in your old Article 25 notifications. You can use this information as a basis for generating your records.

| Old Article 25 | Article 31 of the Regulation |
|---|---|
| (a) | (a), but adding contact details of the DPO and, where applicable, the processor and/or joint controller; |
| (b) | (b) |
| (c) | (c) |
| (d) | removed, but mention this when describing the purposes under (b): in most cases, processing by EUIs will be to accomplish the tasks assigned to them or to comply with obligations under Union legislation; |
| (e) | (d), but more explicit that recipients in third countries / international organisations have to be mentioned as well (mention which ones); |
| (g) | (e) adds information on the safeguards for transfers to third countries / international organisations (e.g. standard contractual clauses, adequacy decision, international treaty) |
| (f) | (f) no specific mention of blocking anymore; mention your conservation periods here (incl. starting date)[27]. |
| (h) | (g) this is only a general description of the measures taken. |

## 5 Positive/negative lists

Please note that these are not yet the official lists under Article 39(4) of the Regulation, but are only meant to provide some guidance in the interim period. The EDPS will keep these lists updated to include any processing operations listed in implementing acts under Article 40(4) as well.

**Positive list of processing operations prima facie requiring a DPIA** (the numbers inside the brackters refer to the criteria in the template threshold assessment in Annex 6 such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (1, 3, 8);

**Indicative list of processing operations prima facie not requiring a DPIA**:

- Management of personal files *as such*[28];
- Standard staff evaluation procedures (annual appraisal);
- 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;

[27] This is to be included 'where possible', but in line with the principle of storage limitation in Article 4(1)(e), your EUI should always be able to name a conservation period ('X years from event Y'). If personal data are lawfully published and public forever, mention this as well.

[28] Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such.

- Establishment of rights upon entry into service;
- Management of leave, flexitime and teleworking;
- Standard access control systems (non-biometric);
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in publicly accessible space).

## 6 Template for threshold assessment / criteria

Before conducting a threshold assessment, check the list in Annex 5. Only proceed to the threshold assessment if your planned processing operations do not fall under that list.

| **I Header** | |
|---|---|
| Name of processing operation | [name] |
| Controller contact point | [name and contact details] |
| Record of processing operations | [record reference] |
| DPO consultation | [date of feedback] |
| Approval | [name and date] |
| **II Criteria for high risks** | |
| *Criterion* | *Applicable? Yes [if so, describe how] / No [if borderline: why not?]* |
| 1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting.<br>*Examples: a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff members based on all their transactions in EUI's case management system with automatic reassignment of tasks.*<br>*Counterexamples: standard appraisal interviews, 360° evaluations for helping staff members develop training plans.* | [Y (how?) / N] |
| 2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects<br>*Example: automated staff appraisal ('if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion')*<br>*Counterexample: a news site showing articles in an order based on past visits of the user.* | [Y (how?) / N] |
| 3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use.<br>*Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption.*<br>*Counterexample: open CCTV of garage entry not covering public space* | [Y (how?) / N] |
| 4. Sensitive data: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive. | [Y (how?) / N] |

| | |
|---|---|
| *Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification*<br>*Counterexample: photos are not sensitive as such (only when coupled with facial recognition or used to infer other sensitive data).* | |
| 5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage:<br>*Examples: European databases on disease surveillance.*<br>*Counterexamples: internal phone directory of an EUI* | [Y (how?) / N] |
| 6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.<br>*Examples: covertly cross-checking access control logs, computer logs and flexitime declarations to detect absenteeism.*<br>*Counterexample: further use of data processed for a grant application when auditing the grant process.* | [Y (how?) / N] |
| 7. Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified.<br>*Examples: children, asylum seekers.*<br>*Counterexample: EUI staff are not automatically considered as vulnerable vis-à-vis their employer concerning standard procedures laid down by the Staff Regulations* | [Y (how?) / N] |
| 8. Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown.<br>*Examples: machine learning, connected cars, social media screening of applicants for posts.*<br>*Counterexamples: 1:1 biometric access control using fingerprints* | [Y (how?) / N] |
| 9. Preventing data subjects from exercising a right or using a service or a contract.<br>*Examples: exclusion databases, credit screening*<br>*Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances)* | [Y (how?) / N] |
| **III Conclusion** | |
| Number of 'Yes' ticked above | [n] |
| Assessment: In general, if you tick two or more of the criteria in the list, you should carry out a DPIA. If you consider that in the specific case at hand, risks are not 'high' even though you have two or more 'yes', explain and justify why you think the processing is in fact not 'high risk'. | [explain] |

# 7 Reference documents

## Guidance on records by EDPB members

Some EDPB members have also published guidance and explanations on how to keep records of processing operations under the functionally equivalent rules of the GDPR:

- Belgian Privacy Commission: explanation (FR/NL) & register template (FR/NL)
- Denmark: Datatilsynet: Vejledning om fortegnelse (January 2018)
- Germany (Datenschutzkonferenz): explanation on registers & template for controllers / processors
- Greece: Hellenic Data Protection Authority: Explanation on registers & templates for controllers / processors.
- UK: Information Commissioner's Office: explanation and template

# 8 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. For more details, see chapter V of the Regulation. |
| 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) of the 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 of the 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 of the 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. Replaced the WP29. |
| European Data Protection Supervisor (EDPS) | The Data Protection Authority for the EUIs (see the Regulation). |
| European Institutions and Bodies (EUIs) | Shorthand for all European Instituions, Bodies, Offices, Agencies and other entities under the scope of the 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 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 |
| (the) Regulation | Regulation (EU) 2018/1725 |
| 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 notificiation | 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 of the 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 of the Regulation) |
| Right of rectification | Data subjects have the right to rectify their personal data held by a controller when they are incorrect (Article 18 of the 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 of the 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 of the Regulation); data concerning criminal convictions and offences (Article 11 of the 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. |