How to Undertake an Information Governance Review for a Project or Process

This resource is aimed at the public sector, and local authorities in particular, but it can be used by any organisation.

This process can be linked to an ethical or equalities review of a project or process.

This process is often used to support Pan-London Data Sharing. Anyone receiving LOTI-led funding will be expected to follow this process and you may find that other funding organisations will expect something similar.

Continuous improvement

Ongoing and regular review of the processing of personal data should be a part of a continuous improvement approach. This is a positive and effective way to consider the risks and benefits to your organisation and the people whose personal data you are processing.

When to undertake a review

Review is particularly important for pilot and research projects where it is likely that there are higher privacy risks and greater uncertainty of how the project will be undertaken, what personal data is involved, or how data subjects will feel about the purposes of processing their data.

A pilot or research project will often meet the criteria for completing a Data Protection Impact Assessment (DPIA). Even without a DPIA, an IG review is most easily done by working through the DPIA structure and assessing each section against what has happened in practice.

You should plan for an IG review at key points in the lifecycle of data use such as:

- ✓ Once you have completed a pilot phase.
- ✓ When a product or system reaches Minimum Viable Product (MVP) or beta testing.
- ✓ When you want to expand the duration or reach of the system or process.
- ✓ When a project ends.

It is useful to complete an IG review as part of the project closure report. This will help you identify ways of working that you want to replicate or approach differently for future projects. The review at project close will also remind you of the retention periods for the data. You can confirm that you have processes for meeting those periods and that data is destroyed or disposed of securely.

Structure of a review report

If you are using a report structure then you may wish to use the following headings:

- **What was in the DPIA?**
- **What has been reviewed?**
- **What are the findings?**
- **Recommendations**

The Review Process

The review must involve the project team or lead, and the DPO (Data Protection Officer) or DP (Data Protection) lead, but can be led by:

- **someone external to the project**
- **someone external to the organisation.**

The output could be a formal report, but as a minimum the review should be documented and provided to the DPO or DP lead, and the project lead.

Activities

1. Identify who will be involved in the review.

2. Agree a timescale for the review and schedule activities. This will help the participants to plan their time.

3. Bring together the relevant documents, which will include any DPIAs, any Data Sharing Agreements (DSAs), risk spreadsheets and project reports. You may want to include contracts, privacy notices, complaints or incident reports.

4. Draft an outline of what you expect to cover:

   a. The original risks.

   b. What the project team/service said they'd do and what they did.

   c. The questions the review will answer.

   d. The documents you expect to read and the analysis you expect the project team to deliver or commission in order to answer the review questions.

   e. Any scope limitations.

5. Confirm the review plan is suitable with the DPO or DP lead, the project team and any relevant stakeholders. Consider whether this is something that a project sponsor or funder needs to formally approve.

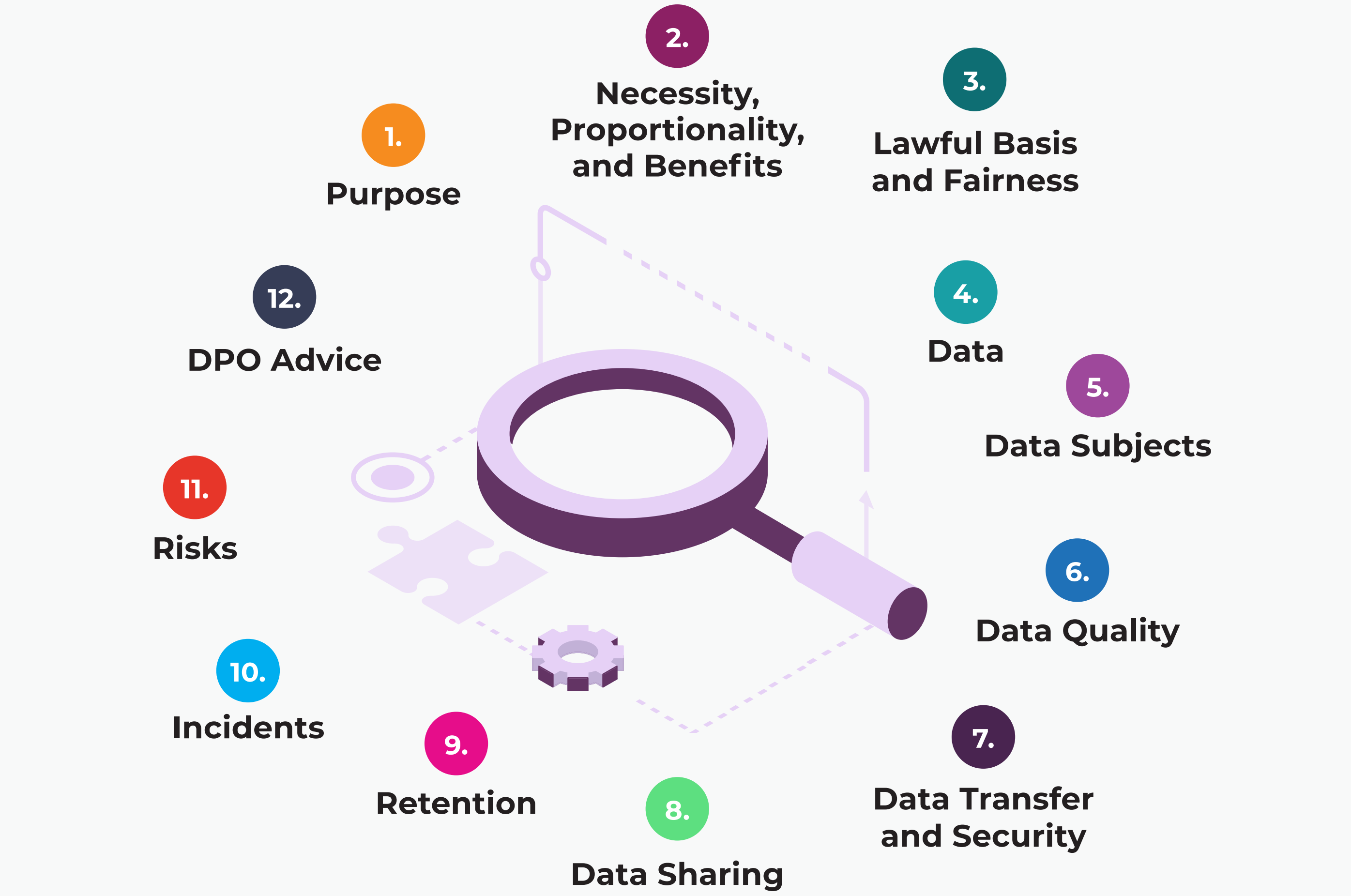
6. Identify if you need interviews, further documents or analysis and send requests for them.

7. Undertake the review using the prompts below and identify any recommendations.

8. Have your draft output/report reviewed by the DPO or DP lead, the project team and any relevant stakeholders.

9. Amend as required based on feedback and create the final output/report.

Review Areas



Review Areas

The review areas follow the structure of a DPIA. Include any relevant evidence in your review report. This may come, for example, from feedback from participants/ data subjects, commendations or complaints, or financial analysis.

1. Purpose

- Has the purpose for processing remained the same?
- Have any new requirements been identified?
- Are the same organisations involved? Explain any change.
- Has your funding source changed?
- Have stakeholders asked for additional or different requirements?
- If you expect the project to move to a new phase or become business-as-usual, what needs to happen to make that possible?

2. Necessity, Proportionality, and Benefits

- Can you still justify that the processing is necessary for the stated purpose(s)?
- Is the processing proportionate? Is there a way of achieving the same or similar benefits whilst processing data in a way that is less intrusive to an individual's privacy?
- Are you achieving or on track to achieve the stated benefits? Do these still balance positively against the privacy intrusion?

3. Lawful Basis and Fairness

- Has any of the applicable legislation or statutory guidance changed? How does that impact the system/process?
- Do the original lawful basis conditions still apply?
- Has your justification for processing changed and how?
- Is the processing still considered fair to data subjects? Have you had any complaints?

4. Data

- Did you use all the data you planned to use?
- Can you reduce the amount or sensitivity of the data?
- Can you anonymise or pseudonymise the data?
- Do you need or want extra data? Why is this necessary and what would it allow you to do?

5. Data Subjects

- Are the data subjects the same?
- Have you adequately explained the processing to them?
- Did they understand the processing? How did they react?
- Did any individuals complain or ask for their data to be deleted or for the processing to stop?
- Did you, or do you need to, change the way you tell individuals about the processing of their data?

6. Data Quality

- Was the data of sufficient quality to allow you to meet your objectives?
- Were you able to match data to a high degree of accuracy?
- Do you need to make changes to the data or the process to improve data quality?
- If data quality issues were discovered, were the parties able to make appropriate changes/updates to data within their systems?
- Were any inappropriate assumptions made about the data or outputs and what happened?
- What changes did you make to improve data quality?

7. Data Transfer and Security

- Did data collection happen according to plan?
- Did the transfer mechanisms work and was data transferred securely?
- Did data remain secure in data storage? Did storage locations or mechanisms change?
- Did the access controls work? Did you need to change who had access to the data or how?

8. Data Sharing

- Did you have a suitable Data Sharing Agreement in place with all relevant parties?
- Did the DSA work as expected?
- Do you need to make any changes and how will you do this?

9. Retention

- Are the stated retention periods appropriate?
- Did secure disposal/destruction of the data happen at the end of the retention period?
- Can you automate retention and destruction?

10. Incidents

- Did any data protection or data security incidents occur?
- Why did these happen?
- What have you done, or what can you do, to reduce the likelihood or severity of potential incidents?

11. Risks

- What were the original concerns?
- Did any of the anticipated risks occur?
- Did an unconsidered issue occur?
- Did you discover new risks and how did you/do you plan to reduce, tolerate or mitigate them?
- Are you able to reduce the risks levels? For example, you can lower the risk for privacy information if during the processing you became more confident that individuals understood what was happening to their data.

12. DPO Advice

- Did you follow all the advice and complete the requirements the DPO stated in the DPIA?
- If not, what did not happen and why?

Recommendations

In light of everything assessed in the IG review, what do the DPO and project team recommend should happen before the project is extended, expanded or repeated?

Close Down Review

If the project or process is ending, adding these considerations to the review report are helpful.

- **Did the processing fit the purpose and were the expected benefits achieved? If not, why not?**
- **Did you receive any requests or complaints from data subjects? How did these affect the project?**
- **Did any data protection or data security incidents occur? How could future projects prevent incidents?**
- **Make recommendations for any actions required with the existing data and project records.**
- **Make recommendations for future projects.**