Managing personal data that you don’t want or need

The third data protection principle (Article 5 (1) (c)) is about data minimisation. Data should be, “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.

Gathering personal data you don’t have a plan for is unlikely to be lawful under data protection legislation.

Data minimisation is a requirement, but it’s also common sense not to gather data that you won’t be using. You will have less data to manage and you’ll be making a small sustainability action to not use energy storing data for no purpose.

Prevention

Start by preventing the collection of data you don’t need.

Establish what you need

- What is the minimum data you need? Be precise - do you need a date of birth or simply an age range?
- Don’t ask questions for the sake of it. If you have not planned the time and resources for analysing the data then you shouldn’t collect it.
- Do not ask for "everything, just in case”.
- Do not expect full system access or whole spreadsheets where you only need some data fields.

Surveys/forms/consultations

- Word your questions and guidance to ask people to exclude data that you don’t want eg “Please do not include any information in your survey comments that may identify you.”
- Remove or reduce free text boxes to prevent unwanted data.
- Don’t automatically ask questions about equalities or contact details if analysing or using this data is not in your project or implementation plan.

Handling unwanted data

However clear you are about what you need, you may receive data that you don't need. This is potentially a data protection breach.

From parties during data matching/sharing

This can happen when someone sends:

- a whole data file when you only need selected fields.
- the wrong data.
- data to the wrong person in your organisation.

What you need to do

- This may be a data breach, so speak to your Data Protection Officer (DPO). Your organisation will have information governance policies for handling potential data protection breaches, which require swift reporting and action.
- Inform the sender of the data; they may need to speak to their DPO about a potential breach.
- Securely delete the unwanted data.
- Look for changes to reduce the likelihood of this happening again. These can include:
    - Changing the process.
    - Changing the wording of a request or template.
    - Introducing an additional step to cleanse/cull data during the sharing process.

Directly from individuals

An individual may give you data that you don't need. This can be more of an issue if data is gathered through an online form that puts data into an automated process, because this may be considered a data protection breach.

For example:

- Automated publication of comments on a planning application, where an individual has included personal data, potentially special category data about their health.
- Someone making an FOI request includes personal data that is automatically published to the council's disclosure log on the website.

What you need to do

- This may be a data breach, so speak to your Data Protection Officer (DPO).
- Remove the data from publication and consider whether you need to move it elsewhere or securely delete it.
- Look for changes to reduce the likelihood of this happening again. This can include:
    - Changing the process.
    - Changing the wording of a request or template.
    - Adding warnings to the start of forms. Consider warning messages

during the process of completing a form eg asking people to check that no unnecessary data is included before clicking the submit button.

When your needs change

To practice data protection by design and default and meet the data minimisation principle, you should establish what data you need before you begin gathering/processing it. However, especially with pilots, you may be genuinely unsure whether some data fields are necessary. It may be possible to justify collecting some data if part of the pilot is a task to establish what data is necessary for your purpose.

This doesn't mean you can gather everything just in case, but there is space for flexibility. You must identify the relevant data fields that will be tested and explain what you will do to establish whether these fields are necessary for your purpose.

It may be necessary for you to collect a data field to allow matching across multiple datasets, even if that field is not going to be used post-match.

When you undertake a Data Protection Impact Assessment (DPIA), your Information Governance team or DPO can provide healthy challenge to identify what is necessary and proportionate.

It is recommended that you review your processing at suitable times, to test whether all data fields are necessary. You may find that some aren't necessary, and perhaps that you need to include some new data fields. Such a review can take place:

- during or at the end of a pilot.
- at regular project meetings.
- before a contract extension or procurement exercise.
- before moving to a new stage of the project or before expanded implementation.

LOTI has guidance on how to complete an information governance review.

When you identify some data is unnecessary

- Review and amend the DPIA and any Data Sharing Agreements (DSAs).
- Change the process, request wording or template and inform people who use them that they have changed.
- Securely delete the unnecessary data.