Checklist 1: What are the duties of the controller?

Processing of personal data needs to adhere to the following principles:

- the processing operation should be lawful, fair and transparent ("**lawfulness**", "**fairness**", "**transparency**");
- the processing operation should be bound to specific purposes ("**purpose limitation**");
- the personal data processed should be adequate, relevant and limited to what is necessary ("**data minimisation**");
- the personal data should be accurate ("**accuracy**");
- the personal data should be kept no longer than necessary ("**storage limitation**");
- the personal data need to be remain well secured and confidential ("**integrity and confidentiality**").

See the EDPS "accountability on the ground" guidance, part II, pages 11-15 for guiding questions on these data protection principles

The controller is responsible for compliance with these principles and should be able to demonstrate this compliance ("principle of accountability"). To achieve this, controllers in practice need to, in particular:

- document their processing operations with **records**
  (note: the EDPS strongly recommends keeping these records in a **central publicly accessible register**);
- carry out a data protection impact assessment (**DPIA**), prior to operations which carry a high risk to the rights and freedoms of data subjects;
- under certain circumstances, **consult the EDPS** prior to such high-risk processing operations;
- when designing processing operations, keep in mind the principles of "**privacy by design**" and "**privacy by default**";
- take **adequate security measures** in order to protect personal data;
- in case of a **personal data breach**, notify the EDPS as well as, under certain circumstances, the data subjects involved;
- conclude **agreements / contracts with processors** (only those providing sufficient guarantees);
- conclude agreements with other controllers in cases of **joint controllership**;
- **transfer** personal data within the EUI, to other EUIs, to third countries or international organisations only when the conditions of the Regulation are complied with;
- **cooperate with the EDPS**.

See the EDPS accountability on the ground for guidance on records, DPIA's, prior consultation and more.

Finally, the controller need to provide **clear and accessible information to data subjects** about the processing, **respect data subject's rights** and ensure their availability in practice.

See the EDPS guidelines on transparency and other rights and obligations.

Know your processing operations

Article 4 of Regulation (EU) 2018/1725 lists the data protection principles. Additional Articles in the Regulation spell them out in more detail:

DP principle	Articles	Recitals
Fairness	*Article 4(1)(a), 17 to 25*	*20, 26, 34, 35, 37-41*
Transparency	*Articles 4(1)(a), 14 to 16, 25*	*20, 35, 36*
Purpose limitation	*Articles 4(1)(b), 6, 13, 38*	*25*
Data minimisation	*Articles 4(1)(c), 12, 13,37, 38*	*20*
Accuracy	*Articles 4(1)(d), 18*	*38*
Storage limitation	*Articles 4(1)(e), 13*	*20, 33*
Security	*Articles 4(1)(f), 33, 36, 37, 39*	*53, 54, 58*

Create a systematic description of the processing. Start from the information you already have in your notification or record and add the following points:

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

Use existing documentation of the process or its development to generate this documentation. Re-read this existing documentation through the lens of "how will this affect the people whose data we process?" and adapt and expand where necessary.

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

The table below maps the targets to some generic processing steps, indicating the most relevant targets for each. These are the **minimum aspects to check**.
Lawfulness is to be ensured as the first stage and at each processing step.

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

See the EDPS "accountability on the ground" guidance, part II, pages 7, 9-11 for mapping data protection principles to generic processing steps