What data is protected?

Describe the data content stored in the system and otherwise used by the system

For example, personal data, grades, financial figures, weather data, temperatures, etc. Outline for yourself the flow of use case data (e.g. the flow of a blood glucose measurement from the client to the medical staff). Remember integrations and logs.

What the data is used for?

What is the purpose of which data?

Note: If you collect personal data, the law requires you to always have a purpose for it. Unnecessary personal data must not be collected.

Where data is stored?

Where and how the data is intended to be stored.

Note: In particular, for the processing of personal data, the location affects the contracts and the protection mechanisms.

What is the life cycle of the data/system?

How long information is stored in the system, who is responsible for managing the information lifecycle.

Often long-term storage is separated into different systems, e.g. in Metropolia into a data warehouse, so be sure to document the data lifecycle in all systems.

Who processes the data?

Who all have access to the data and under what circumstances. Are there roles in the system that have access only to certain data.

For example, usually a student should only have access to the information they need to complete their work.

Who is responsible for which part of the data processing?

Is there an agreement on who is responsible for what in the service provider's services.
Your service provider is exposed to security risks just like any other company, so make sure you have a clear and comprehensive agreement on security and responsibilities.