# Requirements for the Specification and Description of a Target of Evaluation (ToE)

The respective ToE shall be specified and described ("scoping"). The processing operations to be certified must be described in an understandable manner and in complete sentences.[1] A reference to existing documents (e.g. a user manual) is permissible. However, the essential characteristics of the target of evaluation must be mentioned as such in the ToE description. This applies in particular to the following characteristics / aspects:

- List of all parties involved (grouping enables summaries): certification customer (processor), controllers (principals), other processors as well as their sub-service providers (if relevant from a data protection perspective), third parties to whom personal data is disclosed, categories of data subjects such as subscribers, administrators, employees, visitors, prospects, children, customers, suppliers, users of a service, passers-by or patients, and their relationships to the other parties involved (e.g., employees of the processor, administrators at the other processor),
- relevant processes / functionalities and the associated processing operations;
- purposes pursued by the processing operations in each case;
- categories of data subjects and categories of personal data which are the subject of the processing operations concerned;
- Relevant locations (in particular offices of the certification customer and data centres where servers of the customer are located) where personal data may be processed by the customer and / or by (other) processors;
- Technical systems used (hardware, software and infrastructure);
- Interfaces or transitions to other systems and organisations (including underlying protocols and other assurances);
- (Other) processors used by the certification customer, the responsibilities and associated tasks assumed by them (if relevant) and relevant locations in this respect;
- Third parties to whom personal data is disclosed (where relevant);
- Third countries and / or international organisations to which personal data is transferred (where relevant);
- Area of use of the ToE, e.g. use in the healthcare sector and only by healthcare professionals (if the intended use of the ToE is / should be limited to a specific area);
- Meaningful graphical representation of the data flow between the parties or IT systems, naming the data types;

[1] Mere bullet points, on the other hand, are not sufficient.

- Final list of all processing operations covered by the ToE and their core components - a distinction must be made here between the following categories of core components;
- Tabular listing of all processing operations / components that are closely related to the ToE but should not be covered by it[2];
- Description of a use case to guide the evaluation if the target of evaluation allows a variety of uses for different purposes (e.g. cloud-based exchange of digital documents).[3]

Note: The evaluation team of the certification body prepares the description of the target of evaluation, which is binding for the certification procedure. This team takes into account the ToE description provided by the customer as part of the application process, but does not simply continue to use it, instead critically scrutinizing it.

[2] This is the only way to assess whether the envisaged ToE has the necessary significance and represents a self-contained unit. If this is not the case, the ToE cannot be certified in the selected scope. If the selected scope of the ToE is certifiable, the following must be observed: Relevant interfaces must be considered in any case.

[3] The use case must be selected and specified in such a way that particularly high risks that may result from certain uses of the ToE are also considered (e.g. in the case of a cloud-based exchange of digital documents: Exchange of documents containing special categories of personal data).