Requirements for the Implementation of a Maturity Assessment on the Target of Evaluation (ToE)

A so-called maturity assessment shall be carried out. This is to ensure that customers only submit an application for (re)certification if the corresponding ToE and the documentation available for it show a level of maturity from a technical and legal perspective that makes an application appear reasonable (i.e. promising) at the current time. As part of this assessment of the maturity level of the ToE to be certified and the associated documentation as well as the implemented technical and organisational measures, the activities listed below must be carried out:

- Identification of the types of documents required for certification and check that the relevant documents are already available, complete, understandable and up to date;[1]
- Conduct of an analysis of the applicable legislation and listing of all relevant statutory provisions at EU and, where applicable, national level, as well as relevant court rulings and / or guidelines and other interpretative guidance from data protection supervisory authorities;
- Conduct of an analysis of the applicable technical state-of-the-art for the ToE (in this respect, EuroPriSe is guided in particular by the document "Guideline “State of the Art”" by ENISA and TeleTrust)[2];
- Identification and listing of the requirements of the relevant EuroPriSe criteria catalogue that apply to the ToE to be certified[3] (if the target of evaluation includes several processing operations to which different requirements apply, distinct requirement profiles must be established);
- Cursory review and assessment[4] of whether the ToE to be certified can in principle be regarded as certifiable, taking into account the applicable criteria of the respective criteria catalogue, the relevant statutory provisions, the applicable court rulings and the relevant interpretation aids of the supervisory authorities: The purpose of this review is to identify obvious violations of the law and security deficiencies ("showstoppers") in advance of a certification procedure so that the customer can remedy them before submitting the application for certification to the certification body;

---

[1] This includes technical and legal documents (relevant contracts, consent forms, etc.) as well as documents related to other certifications (e.g. ISO/IEC 27001) that are relevant to the certification of the ToE in question in accordance with EuroPriSe. Cf. in this respect the applicable list of relevant documents (as amended from time to time).

[2] https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

[3] Not all requirements are always applicable. For example, some requirements only apply if special categories of personal data are the subject of the ToE to be certified or if they involve a transfer of personal data to third countries.

[4] based on the documentation reviewed, statements made by the certification customer's staff involved in or responsible for the ToE to be certified, and the other results of the risk analysis and the maturity assessment.

- Verification that any identified violations and deficiencies have been successfully addressed.

Note: The purpose of the maturity assessment is not to anticipate a complete examination of the target of evaluation, but to conduct a cursory examination to ensure that the certification body is only confronted with applications for certification if the ToE concerned and its documentation, as well as the technical and organisational measures implemented, have a level of maturity that makes the implementation of a certification procedure appear reasonable / promising.