Anforderungen an die Durchführung eines Maturity Assessments zum Zertifizierungsgegenstand (Target of Evaluation - ToE)

Es muss ein sogenanntes Maturity Assessment (Reifegradbewertung) durchgeführt werden. Damit soll sichergestellt werden, dass Kunden nur dann einen Antrag auf (Re-)Zertifizierung stellen, wenn der entsprechende Zertifizierungsgegenstand und die dazu vorliegende Dokumentation aus technischer und rechtlicher Sicht einen Reifegrad aufweisen, der einen Antrag zum aktuellen Zeitpunkt sinnvoll (d.h. erfolgversprechend) erscheinen lässt. Im Rahmen dieser Reifegradbewertung des ToE und der zugehörigen Dokumentation sowie der umgesetzten technischen und organisatorischen Maßnahmen sind die nachfolgend aufgeführten Tätigkeiten durchzuführen:

- Identifizierung der Arten von Dokumenten, die für die Zertifizierung erforderlich sind, und Überprüfung, ob die relevanten Dokumente bereits vorhanden, vollständig, verständlich und aktuell sind;[1]
- Durchführung einer Analyse der anwendbaren Rechtsvorschriften und Auflistung aller relevanten gesetzlichen Bestimmungen auf EU- und ggf. nationaler Ebene sowie einschlägiger Gerichtsurteile und/oder Leitlinien und sonstiger Auslegungshilfen von Datenschutzaufsichtsbehörden;
- Durchführung einer Analyse zum Stand der Technik im Hinblick auf den Zertifizierungsgegenstand (EuroPriSe orientiert sich dabei insbesondere an dem Dokument "Guideline "State of the Art"" von ENISA und TeleTrust)[2];
- Identifizierung und Auflistung der Anforderungen des relevanten EuroPriSe-Kriterienkatalogs, die für den Zertifizierungsgegenstand gelten (wenn das ToE mehrere Verarbeitungsvorgänge umfasst, für die unterschiedliche Anforderungen gelten, müssen verschiedene Anforderungsprofile erstellt werden)[3];
- Kursorische Prüfung und Bewertung[4], ob der Zertifizierungsgegenstand unter Berücksichtigung der anwendbaren Kriterien des jeweiligen Kriterienkatalogs, der einschlägigen gesetzlichen Bestimmungen, der geltenden Rechtsprechung und der einschlägigen Auslegungshilfen der

[1] Dazu gehören technische und rechtliche Dokumente (z.B. Verarbeitungsverzeichnisse oder relevante Verträge) sowie Dokumente im Zusammenhang mit anderen Zertifizierungen (z. B. ISO/IEC 27001), die für die Zertifizierung des betreffenden ToE nach EuroPriSe relevant sind. Vgl. insoweit die jeweils einschlägige Liste der relevanten Dokumente (in der jeweils gültigen Fassung).

[2] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

[3] Nicht alle Anforderungen sind immer anwendbar. Beispielsweise gelten einige Anforderungen nur, wenn besondere Kategorien personenbezogener Daten Gegenstand des ToE sind oder wenn dieses eine Übermittlung personenbezogener Daten in Drittländer beinhaltet.

[4] auf der Grundlage der geprüften Unterlagen, der Aussagen der Mitarbeiter des Zertifizierungskunden, die an dem Zertifizierungsgegenstand mitwirken oder dafür verantwortlich sind, sowie der sonstigen Ergebnisse der Risikoanalyse und der Reifegradbewertung.

Aufsichtsbehörden grundsätzlich als zertifizierbar angesehen werden kann: Ziel dieser Prüfung ist es, offensichtliche Rechtsverstöße und Sicherheitsmängel ("Showstopper") im Vorfeld eines Zertifizierungsverfahrens zu identifizieren, damit der Kunde diese vor Einreichung des Zertifizierungsantrags bei der Zertifizierungsstelle abstellen kann;

- Überprüfung, ob alle festgestellten Verstöße und Mängel erfolgreich behoben wurden.

Anmerkung: Zweck der Reifegradbewertung ist es nicht, eine vollständige Prüfung des Zertifizierungsgegenstandes vorwegzunehmen, sondern eine kursorische Prüfung durchzuführen, um sicherzustellen, dass die Zertifizierungsstelle nur dann mit Zertifizierungsanträgen konfrontiert wird, wenn das betreffende ToE und seine Dokumentation sowie die umgesetzten technischen und organisatorischen Maßnahmen einen Reifegrad aufweisen, der die Durchführung eines Zertifizierungsverfahrens als sinnvoll / erfolgversprechend erscheinen lässt.