Anforderungen an die Spezifikation und Beschreibung eines Zertifizierungsgegenstands (Target of Evaluation - ToE)

Der jeweilige Zertifizierungsgegenstand muss spezifiziert und beschrieben werden ("scoping"). Die zu zertifizierenden Verarbeitungsvorgänge sind verständlich und in vollständigen Sätzen zu beschreiben.[1] Eine Bezugnahme auf vorhandene Dokumente (z. B. ein Benutzerhandbuch) ist zulässig. Allerdings müssen die wesentlichen Charakteristika des Zertifizierungsgegenstands in der ToE-Beschreibung als solcher erwähnt werden. Dies gilt insbesondere für die folgenden Charakteristika / Aspekte:

- Aufstellung aller Beteiligten (Gruppenbildung ermöglicht Zusammenfassungen): Zertifizierungskunde (Auftragsverarbeiter), Verantwortliche (Auftraggeber), weitere Auftragsverarbeiter sowie deren Sub-Dienstleister (sofern aus Datenschutzsicht relevant), Dritte, gegenüber denen personenbezogene Daten offengelegt werden, Kategorien betroffener Personen wie z. B. Abonnenten, Administratoren, Beschäftigte, Besucher, Interessenten, Kinder, Kunden, Lieferanten, Nutzer eines Dienstes, Passanten oder Patienten und deren Beziehungen zu den anderen Beteiligten (z. B. Beschäftigte des Auftragsverarbeiters, Administratoren beim weiteren Auftragsverarbeiter);
- Relevante Prozesse / Funktionalitäten und die damit einhergehenden Verarbeitungsvorgänge;
- Zwecke, die jeweils mit den Verarbeitungsvorgängen verfolgt werden;
- Kategorien betroffener Personen sowie Kategorien personenbezogener Daten, die Gegenstand der betreffenden Verarbeitungsvorgänge sind;
- Relevante Standorte (insbesondere Büros des Kunden und Rechenzentren, in denen sich Server des Kunden befinden), an denen personenbezogene Daten vom Kunden und / oder von weiteren Auftragsverarbeitern verarbeitet werden (können);
- Verwendete technische Systeme (Infrastruktur, wie etwa Hardware und Software);
- Schnittstellen bzw. Übergänge zu anderen Systemen und Organisationen (einschließlich der zugrundeliegenden Protokolle und sonstigen Zusicherungen);
- Vom Kunden eingesetzte weitere Auftragsverarbeiter, die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben (sofern einschlägig) sowie insoweit relevante Standorte;
- Dritte, gegenüber denen personenbezogene Daten offengelegt werden (sofern einschlägig);

[1] Bloße Stichpunkte reichen hingegen nicht aus.

- Drittländer und / oder internationale Organisationen, an die personenbezogene Daten übermittelt werden (sofern einschlägig);
- Einsatzgebiet des ToE, z. B. Einsatz im Gesundheitsbereich und nur durch medizinisches Fachpersonal (sofern der bestimmungsgemäße Einsatz des ToE auf ein bestimmtes Gebiet beschränkt ist bzw. sein soll);
- Aussagekräftige grafische Abbildung des Datenflusses zwischen den Beteiligten bzw. IT-Systemen unter Nennung der Datenarten;
- Abschließende Auflistung aller Verarbeitungsvorgänge / Funktionalitäten, die Gegenstand des ToE sind;
- Tabellarische Auflistung aller Verarbeitungsvorgänge / Funktionalitäten, die in einer engen Beziehung zum ToE stehen, aber nicht zu diesem gehören sollen[2];
- Beschreibung eines Use Cases, an dem sich die Evaluierung ausrichten soll, falls der Zertifizierungsgegenstand eine Vielzahl von Nutzungsmöglichkeiten zu unterschiedlichen Zwecken zulässt (z. B. cloudbasierter Austausch digitaler Dokumente).[3]

Hinweis: Die für das Zertifizierungsverfahren verbindliche Beschreibung des Zertifizierungsgegenstands wird vom Evaluationsteam der Zertifizierungsstelle angefertigt. Dieses berücksichtigt die vom Kunden im Rahmen der Antragstellung zur Verfügung gestellte ToE-Beschreibung, nutzt diese jedoch nicht einfach weiter, sondern hinterfragt sie kritisch.

[2] Nur so kann nämlich beurteilt werden, ob das anvisierte ToE die nötige Aussagekraft aufweist und eine in sich geschlossene Einheit darstellt. Ist dies nicht der Fall, kann das ToE in dem gewählten Zuschnitt nicht zertifiziert werden. Falls der gewählte Zuschnitt des ToE zertifizierbar ist, ist folgendes zu beachten: Relevante Schnittstellen müssen in jedem Fall mit betrachtet werden.

[3] Der Use Case ist so zu wählen und zu spezifizieren, dass besonders große Risiken, die aus bestimmten Nutzungen des ToE resultieren können, mit betrachtet werden (z. B. im Fall eines cloudbasierten Austauschs digitaler Dokumente: Austausch von Dokumenten, die besondere Kategorien personenbezogener Daten beinhalten).