

Anforderungen an die Durchführung einer Risikoanalyse zum Zertifizierungsgegenstand (Target of Evaluation - ToE)

Zum Zertifizierungsgegenstand muss eine datenschutzspezifische Risikoanalyse durchgeführt werden. Die Ergebnisse dieser Risikoanalyse sind zu dokumentieren.

Im Rahmen der Risikoanalyse

- müssen alle Risiken für die Gewährleistungsziele nach Art. 32(1) DSGVO und für andere Gewährleistungsziele zum Schutz der betroffenen Personen¹ ermittelt werden;
- die Risiken müssen im Hinblick auf ihre Eintrittswahrscheinlichkeit und Schwere bewertet werden; und
- die Risiken müssen mit den technischen und organisatorischen Maßnahmen verglichen werden, die zu ihrer Minimierung getroffen wurden.

Folgende Gewährleistungsziele des Datenschutzes sind im Rahmen einer solchen Risikoanalyse zu berücksichtigen:

- Datenminimierung;
- Verfügbarkeit;
- Integrität;
- Vertraulichkeit;
- Nichtverkettung;
- Transparenz;
- Intervenierbarkeit;
- Belastbarkeit.

Im Rahmen der Risikoanalyse muss auch eine Schutzbedarfseinstufung vorgenommen werden. Dabei ist zu unterscheiden zwischen den Schutzbedarfsklassen

- normal; und
- hoch

Diese Schutzbedarfseinstufung ist dann später insbesondere für die Beantwortung der Frage relevant, ob geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus getroffen wurden.

Im Rahmen der Risikoanalyse ist auch zu prüfen, ob der Zertifizierungsgegenstand Verarbeitungsvorgänge umfasst / zur Folge hat, für die eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchgeführt werden muss.

¹ Vgl. die folgende Liste. In Bezug auf die anderen Gewährleistungsziele basiert das EuroPriSe-Zertifizierungsprogramm auf dem Standard-Datenschutzmodell in seiner jeweils gültigen Fassung.

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