EU-DSGVO

Standard-Datenschutzmodell (SDM)

Relevante Dokumentation

♦ Gesamtes Dokument (Version 2.0, hier Online).
♦ Erprobungsfassung (Version 1.1, hier Online)

Teil A - Beschreibung des Standard-Datenschutzmodells
Teil B - Anforderungen der DSGVO
Teil C - Systematisierung der Anforderungen der DSGVO durch die Gewährleistungsziele
Teil D - Praktische Umsetzung
Teil E - Organisatorische Rahmenbedingungen

Grundlegendes

> Das Standard-Datenschutzmodell ist eine Methode, mit der die Übereinstimmung von Anforderungen des Datenschutzrechts und technisch-organisatorischen Funktionen personenbezogener Verfahren in Deutschland überprüfbar wird. Das SDM soll erstens zu bundesweit abgestimmten, transparenten und nachvollziehbaren Beratungs- und Prüftätigkeiten der Datenschutzbehörden führen und zweitens Organisationen ein Werkzeug an die Hand geben, um selbsttätig personenbezogene Verfahren datenschutzgerecht einrichten und betreiben zu können. (Quelle: Standard-Datenschutzmodell)

Das SDM legt die datenschutzrechtlichen Anforderungen zugrunde, die aus der DSGVO systematisch herausgearbeitet worden sind. Die Anforderungen werden in die drei Blöcke zentrale datenschutzrechtliche Anforderungen, Einwilligungsmanagement und Umsetzung aufsichtsbehördlicher Anforderungen differenziert. Die zentralen datenschutzrechtlichen Anforderungen sind grundsätzlich bei jeder Verarbeitung personenbezogener Daten umzusetzen. Im Einwilligungsmanagement werden die Anforderungen zusammengefasst, die zusätzlich zu erfüllen sind, wenn die Rechtmäßigkeit der Verarbeitung auf Art. 6 Abs. 1 lit. a DSGVO gestützt wird. Schließlich müssen gegebenenfalls für die Umsetzung aufsichtsbehördlicher Maßnahmen weitere Anforderungen berücksichtigt werden. [1)]

Die wesentliche Komponente des SDM besteht aus einem Konzept von sieben elementaren Gewährleistungszielen. Als Gewährleistungsziele gelten die Sicherung der

- Verfügbarkeit,

- Integrität,
- Vertraulichkeit,
- Transparenz,
- Intervenierbarkeit,
- Nicht-Verkettbarkeit, ergänzt um das allgemeine Gewährleistungsziel der
- „Datenminimierung“ (Prinzip der Datensparsamkeit).

Festlegung des Schutzbedarfs aus der Betroffenenperspektive

Das Konzept des SDM sieht vor, diese Gewährleistungsziele heranzuziehen und, in methodischer Anlehnung an IT-Grundschutz des BSI, um Schutzbedarfsfeststellungen zu ergänzen. Im Unterschied zu Grundschutz ist die Schutzperspektive aus der Sicht einzelner Betroffener formuliert und der Schutzbedarf aus der Eingriffsintensität eines personenbezogenen Verfahrens abgeleitet, nicht jedoch aus dem möglichen Schadensrisiko, das aus der Schadenswahrscheinlichkeit und Schadenshöhe errechnet wird.

Bezug des SDM zum IT-Grundschutz und zu ISO-Normen

Das SDM ist auch im IT-Grundschutz direkt verankert: Im Abschnitt zu Datenschutz weist das BSI darauf hin, dass die Nichtberücksichtigung des SDM begründet werden müsse.

Die Vorgaben einer Datenschutzprüfung ergeben sich aus dem Datenschutzrecht. Datenschutzanforderungen haben einen sehr viel höheren Verpflichtungsgrad als Anforderungen der IT-Sicherheit, wie sie bspw. vom IT-Grundschutz des BSI oder von Normen der ISO formuliert werden. Ohne eine Rechtsgrundlage dürfen Organisationen keine Personendaten verarbeiten.

Dieses grundlegende Verbot mit Erlaubnisvorbehalt entspricht der grundlegenden „Firewall-Regel“, wonach zunächst alle Ports zu schließen sind (*Deny-All*); anschließend werden nur die unverzichtbaren Ports für Kommunikationsverbindungen bzw. die notwendige Datenverarbeitung geöffnet.

Deshalb beginnt jede Datenschutzprüfung personenbezogener Verfahren mit der Prüfung der Rechtsgrundlagen, die eine zweckdefinierte Verarbeitung legitimieren. Trägt diese Rechtsgrundlage, können Soll-Vorgaben an eine datenschutzgerechte Datenverarbeitung mit technisch-organisatorischen Schutzmaßnahmen formuliert und mit den Ist-Feststellungen einer Bestandsaufnahme vor Ort verglichen bzw. beurteilt werden.

Datenlizenz

1)

Auszug aus Teil B