**A.1 - Datenschutz-Vorgehensmodell (für öffentliche Stellen)**
(analog BSI 200-1)
Stand: 11.07.2022
Version 1.2

1. Datenschutz-Grundsätze

* Grundsatz der Rechtmäßigkeit (Art. 5, 6 DSGVO; Art. 20 Abs. 3 GG, §§ 3, 25 NDSG, Rechtsgrundlagen ausgerichtet auf öff. Stellen, Besonderheiten ggü. nicht-öffentlichen Stellen)
* Verarbeitung personenbezogener Daten nur mit ausreichender Legitimation (Gesetz/Einwilligung)
* Grundsatz der Transparenz und Wahrung der Betroffenenrechte, der Datenminimierung
* Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
* Grundsatz der Datensicherheit

2. Informationsverbund in Strukturanalyse festlegen

* Nur mit Definition der Gesamtheit und Einzelheiten der Datenverarbeitung (ZAWAS: Strukturanalyse) kann Prüfung erfolgen
* Betroffene und die jeweils betroffenen personenbezogenen Daten identifizieren
* Art, Umfang, Umstand und Zweck der Datenverarbeitung
* Inhalte des Verzeichnisses der Verarbeitungstätigkeiten (VVT) (Muster)
* Gesetzliche (Mindest-)Inhalte zzgl. Rechtsgrundlage
* Festlegung der Schutzstufe (A-E bzw. 1-3)
* Prüfung der Rechtmäßigkeit / der Rechtsgrundlage
* Gewährleistung der Datensicherheit, Belastbarkeit etc.
* Prüfung der ursprünglichen Zweckbindung und -einhaltung

3. Risikobewertung vornehmen

* Innerhalb der Risikobewertung ist bereits ein allgemeines Risikoniveau enthalten, dem durch Basis-TOM begegnet werden kann.
* Es sind die Risiken für Rechte und Freiheiten natürlicher Personen in einer Risikoanalyse zu bewerten (nicht die Risiken für das Unternehmen, die Behörde —> nicht der Verantwortlichen. Diese anderen Risiken sind ggf. in einer separaten Risikobewertung zu betrachten)
* Anhand von standardisierten Risiken sind die notwendigen technischen und organisatorischen Maßnahmen aus den (Basis-TOM) zu identifizieren

4. Risikobehandlung

* Festlegung notwendiger TOM konkret bezogen auf festgestellte Risiken (ggf. erweiterte Maßnahmen über Basis-TOM hinaus)
* Schwellenwertanalyse (Ergänzende Risikoanalyse - liegt trotzdem ein hohes Risiko vor?) (ggf. Einbindung LfD)
* Tragung des Restrisikos (unabhängig von DSFA)

5. Ggf. Datenschutz-Folgenabschätzung

* Mindestinhalte aus Gesetz / WP 248

6. Betroffenenrechte wahren

* Differenzierung nach Betroffenengruppen aus VVT (Kunden/Kundinnen / Beschäftigte / Dritte)
* Auskunft, Berichtigung, Löschung, Data Breach, Information bei Erhebung
* ggf. Berücksichtigung innerhalb der Datenschutz-Folgenabschätzung (Art. 35 Abs. 9 DSGVO - Personalvertretung?)

7. Privacy by design/Default

* Grundsatz der Datenminimierung im Entwurf der Verarbeitungstätigkeit und der technischen Umsetzung implementiert

8. Realisierung/Überprüfung