TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Methodiken zur Risikoanalyse in der Datenschutz-Folgenabschätzung (DSFA)

Jens Syckor / Thorsten Strufe / Anne Lauber-Rönsberg

Jahreskonferenz Forum Privatheit 2022

Berlin / 14.10.2022

Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO

- Durchführungspflicht für den Verantwortlichen bei Formen der Verarbeitungen mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen
- vor Einführung Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz personenbezogener Daten

DSFA enthält zumindest:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck
- **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren.

Untersuchungsgegenstand

- Risiken ausgewählter Use-Cases und Abbildung auf Anforderungen in der DSGVO
- Adressierung dieser Anforderungen bei ausgewählten Methodiken

- Analysefähigkeit der Methodiken bzgl. der Risiken
- Herausforderungen bei der Anwendbarkeit der Methodiken
- Einsatzbereich und Voraussetzungen beim Verantwortlichen (Softwareentwicklung, Datenschutzbeauftragte, externe Unterstützung)

Ausgewählte Use-Cases und Methodiken

Use-Cases

- Datenverarbeitungen im Kontext von Big Data Analytics mit hohem Risiko,
- Softwareentwicklung am Beispiel der Corona-Warn-App (CWA) Deutschland,
- Einsatz von Software-as-a-Service-Lösungen (SaaS) aus der Cloud von marktüblichen großen Anbietern (Microsoft, Google)

Methodiken

- Ansatz Fraunhofer ISI auf Basis des Standard-Datenschutzmodells (SDM),
- Privacy Impact Assessment (PIA) der CNIL,
- LINDDUN,
- NIST Privacy Risk Assessment Methodology (PRAM)

Abbildung Risikoszenarien auf die DSGVO

- Risiken sind abbildbar auf Grundsätze der Datenverarbeitung gemäß Art. 5 Abs. 1 DSGVO:
  - Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit (sowie implizit Verfügbarkeit)
- Risiken entstehen:
  - a) aus der Verarbeitung selbst bzw. b) aus Abweichungen von den Grundsätzen
- Risikoszenarien aus b) könnten mit Bedrohungsanalysen oder ähnlichen Vorgehensweisen modelliert werden
- **Fazit:** DSFA-Methodiken müssen die Grundsätze der Datenverarbeitung aus Art. 5 Abs. 1 DSGVO oder Teilbereiche davon abbilden

Abbildung Risikoszenarien zur DSGVO

Grundsatz Art. 5 DSGVO	PIA (CNIL)	Fraunhofer ISI (SDM)	LINDDUN	NIST PRAM
Transparenz	(*)	*	*	(*)
Zweckbindung	(*)	*	*	(*)
Datenminimierung	(*)	*	*	(*)
Richtigkeit	(*)	*	*	(*)
Speicherbegrenzung	(*)	*	*	(*)
Integrität	*	*	*	(*)
Vertraulichkeit	*	*	*	(*)

Herausforderungen Risikoszenarien

Grundsatz Art. 5 DSGVO	PIA (CNIL)	Fraunhofer ISI (SDM)	LINDDUN	NIST PRAM
Transparenz	!	!	!	!
Zweckbindung	!	! (Nicht-Verkettbarkeit)		!
Datenminimierung	!		!	!
Richtigkeit	!		!	!
Speicherbegrenzung	!		!	!
Integrität		!	-	!
Vertraulichkeit		!		!

- PIA: Risikomodell nur für Datensicherheit
- SDM: Komplexität insb. durch Spannung zwischen Gewährleistungszielen
- LINDDUN: Nutzung in der Softwareentwicklung
- PRAM: Anpassung auf die DSGVO notwendig