Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

5.12.2017

# Hinweise zur Datenschutz-Folgenabschätzung nach Art. 35 Datenschutz-Grundverordnung

Die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist Ausdruck des risikobasierten Ansatzes der Datenschutz-Grundverordnung. Durch die Datenschutz-Folgenabschätzung (DSFA) sind Verarbeitungsvorgänge, die ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen bergen, vorab auf ihre Folgewirkungen für deren Persönlichkeitsschutz zu überprüfen.

**Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?**

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 DS-GVO in vier Fällen vorgeschrieben:

- wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat,
- wenn umfangreich besondere Kategorien personenbezogener Daten verarbeitet werden,
- wenn Profiling- und Scoring-Verfahren zum Einsatz kommen oder
- wenn eine systematische und umfassende Überwachung öffentlich zugänglicher Bereiche erfolgt.

Der erste Fall basiert auf dem Ergebnis einer vorherigen Risikoanalyse, wie sie in Art. 25 und Art. 32 DS-GVO vorgeschrieben ist. In den übrigen Fällen geht die Datenschutz-Grundverordnung aufgrund der Art der Verarbeitung pauschal von einem bestehenden hohen Risiko aus.

Für bestehende Datenverarbeitungen ist eine Datenschutz-Folgenabschätzung dann nicht durchzuführen, wenn diese einer Vorabkontrolle unterzogen wurden und sich keine wesentlichen Änderungen ergeben haben. Sie ist hingegen durchzuführen, wenn sich seit der Vorabkontrolle Änderungen ergeben haben, die voraussichtlich mit einem hohen Risiko verbunden sind.

Eine Datenschutz-Folgenabschätzung kann für mehrere Datenverarbeitungstätigkeiten durchgeführt werden, die nach Art, Reichweite, Kontext, Zweck und Risiken vergleichbar sind.

**Was sind die Rechte und Freiheiten, für die ein voraussichtlich hohes Risiko zu prüfen ist?**

Als Rechte und Freiheiten natürlicher Personen, für die ein etwaiges hohes Risiko zu prüfen ist, sind insbesondere folgende Rechte der Europäischen Grundrechtecharta von Bedeutung:

- das Recht auf Schutz personenbezogener Daten (Art. 8 EU GR-Charta),
- das Recht auf Achtung des Privat- und Familienlebens (Art. 7 EU GR-Charta),
- das Recht auf Meinungs- und Informationsfreiheit (Art. 11 EU GR-Charta),
- die Gedanken-, Gewissens- und Religionsfreiheit (Art. 10 EU GR-Charta),
- das Recht auf Nichtdiskriminierung (Art. 21 EU GR-Charta).

**Was muss eine Datenschutz-Folgenabschätzung beinhalten?**

Nach Art. 35 Abs. 7 DS-GVO muss eine Datenschutz-Folgenabschätzung mindestens Folgendes enthalten:

- eine Beschreibung der Verarbeitungsvorgänge und die Zwecke der Verarbeitung, sowie
- die vom Verantwortlichen verfolgen berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die o.g. Rechte und Freiheiten,
- die zur Kompensation der Risiken vorgesehenen Maßnahmen.

**Wie ist eine Datenschutz-Folgenabschätzung durchzuführen?**

Der Zusammenschluss der europäischen Datenschutzbeauftragten, die Art. 29-Gruppe, hat im Oktober 2017 Leitlinien zur Datenschutz-Folgenabschätzung veröffentlicht (s.u. „Links“). Darin in ist als methodische Grundlage für die Durchführung einer Datenschutz-Folgenabschätzung ausdrücklich das von der Datenschutzkonferenz empfohlene Standard-Datenschutzmodell genannt.

Die darin zugrunde gelegten Gewährleistungsziele bieten sich daher insbesondere für eine Konkretisierung der Risikobereiche für das Recht auf Schutz personenbezogener Daten an:

- Datensparsamkeit
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettbarkeit
- Transparenz
- Intervenierbarkeit

Hinsichtlich der für die technisch-organisatorischen Aspekte relevanten Gesichtspunkte können für die Risikoanalyse sowie die zu treffenden Maßnahmen der BSI-Standard 200-3 (Risikomanagement) und das IT-Grundschutzkompendium herangezogen werden.

**Wann ist voraussichtlich ein hohes Risiko gegeben?**

Die genannten Leitlinien enthalten folgende Kriterien, die für die Annahme eines hohen Risikos sprechen:

- eine umfangreiche Verarbeitung personenbezogener Daten (nach Datenumfang, Anzahl der Betroffenen, Dauer der Verarbeitung/Speicherung oder geografischer Reichweite),
- eine Verknüpfung von Datenbeständen, die für unterschiedliche Zwecke erhoben wurden,
- eine Verarbeitung von Daten schutzbedürftiger Personen (z.B. Beschäftigte, Patienten, Schutzsuchende),
- der Einsatz innovativer Verarbeitungstechniken (z.B. biometrischer Gesichtserkennung, -analyse).

**Wann ist die Aufsichtsbehörde zu beteiligen?**

Nach Art. 36 DS-GVO ist die Aufsichtsbehörde zu beteiligen, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft oder treffen kann.

**Was sind die Konsequenzen, wenn eine erforderliche Datenschutz-Folgenabschätzung nicht durchgeführt wird?**

Ein Verstoß gegen die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist nach Art. 83 Abs. 4 Buchstabe a) DS-GVO bußgeldbewehrt.

***Links:***

***Leitlinie der Art. 29-Gruppe zur Datenschutzfolgeabschätzung (Deutsche Fassung)***
*WP248:*
*https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/wp243rev01_de.pdf*
*Anhang:*
*https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/wp243rev01_annex_de.pdf*

***Standard-Datenschutzmodell:***
*https://www.datenschutz.rlp.de/de/themenfelder-themen/standard-datenschutzmodell/*