Checkliste

Muss Ihr Unternehmen eine Datenschutz-Folgenabschätzung (DSFA) durchführen?

Eine Checkliste von

COMP/LEX
BERATUNG IM IT-RECHT

1. **Wurde ein neues Verfahren der Verarbeitung personenbezogener Daten implementiert oder ein bestehendes Verfahren wesentlich geändert?**
    - **Ja:** Weiter prüfen unter Ziffer 2, ob eine DSFA notwendig ist.
    - **Nein:** Keine DSFA erforderlich.
    - **Hinweis:** Bei geringfügigen Änderungen könnte eine „light"-Version der DSFA ausreichen. Risiken für die Rechte und Freiheiten natürlicher Personen durch die Verarbeitung sollten immer überprüft werden.

2. **Ist eine gültige Rechtsgrundlage für die Verarbeitung vorhanden?**
    - **Ja:** Überprüfung der weiteren Voraussetzungen ab Ziffer 3.
    - **Nein:** Verarbeitung unzulässig. Eine DSFA ist in diesem Fall nicht mehr notwendig.
    - **Hinweis:** Die Verarbeitung muss auf eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO gestützt werden können (z. B. Einwilligung, Vertragserfüllung, berechtigtes Interesse etc.).

3. **Ist die Verarbeitung auf der Whitelist der Aufsichtsbehörden genannt?**
    - **Ja:** Keine DSFA erforderlich.
    - **Nein:** Weiter prüfen.
    - **Hinweis:** Eine Whitelist legt fest, bei welchen Verfahren keine DSFA erforderlich ist. Derzeit gibt es jedoch **keine** solchen Whitelists.

4. **Wurde bereits eine DSFA für einen vergleichbaren Verarbeitungsvorgang mit ähnlichem Risiko durchgeführt?**
    - **Ja:** Möglichkeit, auf die bestehende DSFA in Teilen zu verweisen. Eine genaue Dokumentation ist erforderlich.
    - **Nein:** Weiter prüfen mit Ziffer 5.
    - **Hinweis:** Der Datenschutzbeauftragte (DSB) sollte im Einzelfall die Vergleichbarkeit prüfen und dokumentieren.

5. **Ist die Verarbeitung auf der Blacklist/Positivliste der Datenschutzkonferenz (DSK) oder der Aufsichtsbehörden genannt?**
    - **Ja:** Eine DSFA ist in jedem Fall erforderlich.
    - **Nein:** Weiter prüfen mit Ziffer 6.
    - **Hinweis:** Die Blacklist enthält Verarbeitungsvorgänge, bei denen ein hohes Risiko besteht und eine DSFA durchgeführt werden muss.

6. **Hat die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen?**
    - **Ja:** Eine DSFA ist erforderlich.
    - **Nein:** Keine DSFA erforderlich, aber dies sollte dokumentiert werden.
    - **Hinweis:** Prüfen Sie insbesondere die Regelbeispiele aus Art. 35 Abs. 3 DSGVO (z. B. Profiling, Verarbeitung besonderer Kategorien personenbezogener Daten, Überwachung öffentlich zugänglicher Bereiche). Nutzen Sie auch die Erwägungsgründe 75, 89, 91 und 76 zur Risikoabschätzung.

7. **Verwendung von künstlicher Intelligenz (KI) oder Chatbots:**
    - **Ja:** Prüfen, ob eine DSFA notwendig ist (z. B. bei komplexen Chatbot-Systemen oder der Verwendung von KI zur Interaktion mit Nutzern).
    - **Nein:** Keine DSFA erforderlich, aber Gründe für diese Entscheidung dokumentieren.
    - **Hinweis:** Bei einfacher strukturierten Systemen ist die DSFA eventuell auch bei KI-Nutzung nicht erforderlich, aber dies sollte gut begründet und dokumentiert werden.

Zusätzliche Hinweise:

- **Dokumentation:** Auch wenn keine DSFA notwendig ist, müssen die Gründe dafür dokumentiert werden, um die Rechenschaftspflicht nach der DSGVO zu erfüllen.
- **Unterstützung:** Der Datenschutzbeauftragte (DSB) kann bei der Risikobewertung und der DSFA-Entscheidung helfen.