

# **DSFA**

—

## **Worauf Kommunen achten müssen**

Stand: April 2021

## Datenschutz-Folgenabschätzung - auch bei Bestandsverfahren

**Besteht bei einer Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person, so muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Dies gilt auch für Bestandsverfahren, die schon lange in Einsatz sind. Die Frist dafür läuft am 25. Mai 2021 ab.**

Doch nicht für jedes Verfahren ist eine DSFA erforderlich. Bei der Prüfung der Erforderlichkeit hilft ein Prüfschema des bayerischen Landesbeauftragten für Datenschutz (BayLfd). Wichtig für AKDB-Kunden ist dabei die Frage, ob eine Vorwegnahme einer DSFA im Sinne von Art. 14 BayDSG erfolgt ist. Im Klartext: wenn eine öffentliche Stelle wie die AKDB ein Verfahren entwickelt und dafür eine DSFA erstellt hat, kann diese übernommen werden.

Die **Erforderlichkeitsprüfung** ist schriftlich zu dokumentieren, am besten mit Hilfe des Formblatts, das der BayLfd auf seiner Website zur Verfügung stellt.

## Die Datenschutz-Folgenabschätzung

Ist eine DSFA notwendig, so wird in einer Risikoanalyse ermittelt, ob die Datenverarbeitung die Ziele des Standard-Datenschutzmodells (SDM) erfüllt. Es werden Risikoszenarien erarbeitet und Maßnahmen definiert, die das Risiko minimieren. Aus der Risikoanalyse ergibt sich eine Gesamtrisikobewertung, die in einen DSFA-Bericht einfließt, ebenso wie die Maßnahmen zur Risikominimierung.

Ein Formular für den DSFA-Bericht, ein Muster für eine Risikoanalyse und ein praktisches Beispiel dazu sind auf der Website des BayLfd zu finden.

## Besonderheiten bei AKDB-Verfahren

AKDB-Verfahren enthalten viele voreingestellte datenschutzkonforme Funktionen, die in der Risikoanalyse und im DSFA-Bericht aufgezeigt werden. Um aber einen wirksamen, datenschutzgerechten Betrieb der AKDB-Verfahren vor Ort zu gewährleisten, müssen die vorhandenen Funktionen aktiviert werden. Auch gibt es Maßnahmen zu Schutz und Sicherheit der Daten, die nur vor Ort getroffen werden können, z. B. die Gewährleistung der Gebäudesicherheit oder der Umgang mit Betroffenenrechten. All dies ist in einem Beiblatt zum DSFA-Bericht aufgeführt. Das Ausfüllen dieses Beiblatts und die Bestätigung der wirksamen Umsetzung der Schutzmaßnahmen ist Aufgabe der Kommunen.

AKDB-Verfahren können sowohl im zertifizierten AKDB-Rechenzentrum (ISO 27001-Zertifikat auf Basis von IT-Grundschutz), als auch autonom vor Ort auf den Servern einer Kommune betrieben werden.

Für jede Betriebsart ist ein gesonderter DSFA-Bericht mit Beiblatt nötig. Bei autonomem Betrieb eines AKDB-Verfahrens ist die Liste der Maßnahmen, die vor Ort getroffen werden müssen, deutlich länger als bei Betrieb im AKDB-Rechenzentrum. Denn dort gewährleistet die AKDB viele Maßnahmen zum Schutz der Daten, die bei autonomem Betrieb von der Kommune selbst getroffen werden müssen.

## Zusammenfassung

In der **Erforderlichkeitsprüfung** wird untersucht, ob eine Datenschutz-Folgenabschätzung notwendig ist. Ist das Ergebnis, dass eine **Datenschutz-Folgenabschätzung** durchzuführen ist, so sind ein DSFA-Bericht und eine Risikoanalyse zu erstellen.

Ein Prüfschema für die Erforderlichkeitsprüfung mit einem Formblatt zur Dokumentation, ein Muster-DSFA-Bericht und ein Beispiel für eine Risikoanalyse sind auf der Website des Bayerischen Landesbeauftragten für Datenschutz zu finden (<https://www.datenschutz-bayern.de/dsfa/>)

Bei **AKDB-Verfahren** erstellt die AKDB für ihre Kunden die DSFA-Berichte und die Risikoanalyse sowie das Beiblatt. Die Kommune, die das AKDB-Verfahren einsetzt, füllt das Beiblatt aus und bestätigt damit, dass sie vor Ort wirksame Maßnahmen zu Schutz und Sicherheit der Datenverarbeitung getroffen hat.

Die Innovationsstiftung Bayerische Kommune hat die Gesellschaft für kommunalen Datenschutz mbH (GKDS) beauftragt, ein Webinar zur DSFA zu erstellen. Es kann auf der Website der Innovationsstiftung <https://www.bay-innovationsstiftung.de/> abgerufen werden.