GKDS

Ihr Partner für kommunalen Datenschutz

Datenschutz-Folgenabschätzung

Was ist zu tun?

Stand: April 2021

Als im Mai 2018 die europäische Datenschutzgrundverordnung (DSGVO) in Kraft trat, enthielt sie eine wichtige Neuerung in Art. 35 DSGVO: die Datenschutz-Folgenabschätzung (DSFA). Besteht bei einer Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person, so muss der für diese Datenverarbeitung Verantwortliche eine Datenschutz-Folgenabschätzung durchführen.

Dies gilt nicht nur für zukünftig geplante Datenverarbeitungen, sondern auch für bereits laufende, die ohne wesentliche Änderungen fortgeführt werden. Bei diesen Bestandsverfahren löst die Datenschutz-Folgenabschätzung die bisherige datenschutzrechtliche Freigabe nach Art. 26 BayDSG (alt) ab. Bis zum 25.Mai 2021 ist zu prüfen, ob eine DSFA erforderlich, und diese gegebenenfalls nachzuholen ist.

Die Erforderlichkeitsprüfung

Nicht für jedes bisher freigabepflichtige Verfahren ist künftig eine Datenschutz-Folgenabschätzung (DSFA) notwendig. In einem ersten Schritt wird deshalb die Erforderlichkeit einer DSFA geprüft. Dazu kann das Prüfschema in der Orientierungshilfe des bayerischen Landesbeauftragten für Datenschutz (BayLfD) herangezogen werden. Darin wird beispielsweise abgefragt, ob es einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken gibt, für den bereits eine DSFA durchgeführt wurde oder ob das Verfahren auf der Bayerischen Blacklist des BayLfD aufgeführt ist.

Gegebenenfalls muss eine eigene Risikoabschätzung nach den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)" der europäischen „Datenschutzgruppe nach Artikel 29" erstellt werden. Darin wird u. a. geprüft, ob der Verarbeitungsvorgang die Beobachtung oder Kontrolle von Personen zum Ziel hat oder ob vertrauliche Informationen verarbeitet werden.

Auch wenn man nach gründlicher Prüfung zu dem Schluss kommt, dass keine DSFA durchzuführen ist, ist die Erforderlichkeitsprüfung schriftlich zu dokumentieren und bei einer Prüfung der Aufsichtsbehörde vorzulegen. Ein Formblatt zur Dokumentation befindet sich auf der Website des BayLfD.

Die Datenschutz-Folgenabschätzung

Der Erforderlichkeitsprüfung folgt bei positivem Ergebnis in einem zweiten Schritt die DSFA. Es wird in einer Risikoanalyse ermittelt, ob die Datenverarbeitung die Ziele des Standard-Datenschutzmodells der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erfüllt. In der Risikoanalyse werden Risikoszenarien erarbeitet und Maßnahmen definiert, die dem Risiko entgegenwirken. Das Ergebnis der Risikoanalyse und die Maßnahmen fließen in einen Bericht ein, der Bestandteil jeder DSFA ist.

Ein Formular für den DSFA-Bericht und ein Muster für eine Risikoanalyse ist auf der Website des LfD zu finden, ebenso wie das Dokument „Datenschutz-Folgenabschätzung – Methodik und Fallstudie", in dem das Vorgehen bei Erstellung einer DSFA detailliert beschrieben ist.

Besonderheiten bei AKDB-Verfahren

In Art. 14 BayDSG (neu) sind Fälle beschrieben, in denen eine DSFA unterbleiben kann. Art. 14 Absatz 2 BayDSG (neu) legt fest, dass eine öffentliche Stelle, die ein automatisiertes Verfahren entwickelt, das zum Einsatz durch öffentliche Stellen bestimmt ist, die DSFA durchführen kann und diese kann dann von einer öffentlichen Stelle, die das Verfahren im Wesentlichen unverändert betreibt, übernommen werden. Wenn also eine Kommune z. B. im Meldeamt ein AKDB-Verfahren, einsetzt, so muss sie keine eigene DSFA durchführen, sondern kann diejenige der AKDB übernehmen.

AKDB-Verfahren enthalten viele voreingestellte datenschutzkonforme Funktionen. Um einen wirksamen, datenschutzgerechten Betrieb dieser Verfahren vor Ort zu gewährleisten, müssen diese Funktionen aktiviert werden. Weitere Maßnahmen zu Schutz und Sicherheit der Daten können nur vor Ort getroffen werden, z. B. die Gewährleistung der Gebäudesicherheit oder der Umgang mit Betroffenenrechten. Diese Maßnahmen listet die AKDB in einem Beiblatt zum DSFA-Bericht auf. Dieses Beiblatt füllen die Kommunen aus und bestätigen damit die wirksame Umsetzung der Schutzmaßnahmen. Sie fügen es den relevanten Datenschutzdokumenten bei und legen es bei einer Prüfung der Aufsichtsbehörde vor.

Beim Betrieb der AKDB-Verfahren gibt es zwei Varianten:

- Verfahren, die im zertifizierten Rechenzentrum der AKDB (ISO 27001-Zertifikat auf Basis von IT-Grundschutz) betrieben werden,
- Verfahren, die autonom in der Kommune vor Ort im eigenen Serverraum oder Rechenzentrum betrieben werden.

Für jede der beiden Varianten stellt die AKDB unterschiedliche DSFA-Berichte und Beiblätter zur Verfügung. Bei autonomen Betrieb der AKDB-Verfahren ist die Liste der Maßnahmen im Beiblatt deutlich länger als bei Rechenzentrumskunden der AKDB. Denn in ihrem eigenen Rechenzentrum trifft die AKDB die betriebstechnischen Maßnahmen zum Schutz der Datenverarbeitung, während bei autonomen Betrieb die Kommune diese Maßnahmen selbst treffen muss.

Zusammenfassung

In der Erforderlichkeitsprüfung wird festgestellt, ob eine Datenschutz-Folgenabschätzung notwendig ist. Ein Prüfschema für die Erforderlichkeitsprüfung und ein Formblatt zur Dokumentation stellt der Landesbeauftragte für Datenschutz in Bayern auf seiner Website zur Verfügung.

Ergibt die Erforderlichkeitsprüfung, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, so sind ein Bericht und eine Risikoanalyse zu erstellen. Ein Formblatt für den DSFA-Bericht und ein Beispiel einer Risikoanalyse sind ebenfalls auf der Website des Bayerischen Landesbeauftragten für Datenschutz zu finden.

Link zur Datenschutz-Folgenabschätzung auf der Website des Bayerischen Landesbeauftragten für Datenschutz: https://www.datenschutz-bayern.de/dsfa/

Bei **AKDB-Verfahren** erstellt die AKDB die Datenschutz-Folgenabschätzung und stellt sie zur Verfügung. Die DSFAs der AKDB enthalten ein Beiblatt, in dem die Kommune bestätigt, dass sie wirksame Maßnahmen zu Schutz und Sicherheit der Datenverarbeitung vor Ort getroffen hat.

Sie haben Fragen zur Erforderlichkeitsprüfung oder zur Datenschutz-Folgenabschätzung? Sprechen Sie uns an, wir beraten Sie gerne.

Kontakt:

GKDS – Gesellschaft für kommunalen Datenschutz mbH
80686 München, Hansastraße 12-16
Tel.: 089 /547 58-0
kontakt@gkds.bayern
www.gkds.bayern