



Informationsblatt

Schwellwertanalyse bei Einträgen des Verzeichnisses der Verarbeitungstätigkeiten

Rechtliche Grundlage zur Datenschutzprüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach Art. 58 der Datenschutz-Grundverordnung (DS-GVO) die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich im Bundesland Bayern, d. h. in privaten Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden. Zu diesem Zweck führt das BayLDA auch flächendeckende Prüfungen zu verschiedenen Schwerpunktthemen durch, bspw. um grundlegende Sicherheitslücken oder organisatorische Defizite aufzuzeigen und Verantwortliche somit auf den Bedarf an durchzuführenden Maßnahmen hinzuweisen. Auch wenn der vorbeugende Charakter der Datenschutzkontrollen des BayLDA hervorgehoben wird, besteht grundsätzlich weiterhin die Möglichkeit, bei Datenschutzverstößen Geldbußen gegen Verantwortliche zu verhängen.

Schwellwertanalyse

Die Datenschutzgrundverordnung hat mit der Datenschutzfolgenabschätzung (DSFA) ein neues Instrument zum Umgang mit Hochrisikoverarbeitungen personenbezogener Daten eingeführt. Diese ist nach Art. 35 Abs. 1 DS-GVO dann durchzuführen, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Damit besteht eine Datenschutzfolgenabschätzung bei Blick auf eine Verarbeitung nach Art. 30 Abs. 1 DS-GVO (Verzeichnis der Verarbeitungstätigkeiten - VVT) aus zwei Schritten:

1. Prüfung, ob für einen Eintrag des VVT eine Datenschutzfolgenabschätzung durchgeführt werden muss. Dies nennt sich auch **Schwellwertanalyse**.
2. Hat die Schwellwertanalyse ein voraussichtlich hohes Risiko ergeben, dann muss eine DSFA durchgeführt werden.

Bei der **Durchführung einer Schwellwertanalyse** ist in der Regel folgendes Vorgehen angebracht:

1. Prüfung, ob der Eintrag des VVT in die Beispiele des Art. 35 Abs. 3 DS-GVO fällt.
2. Falls nicht, Prüfung ob der Eintrag des VVT in die sog. Muss-Liste zur DSFA der DSK fällt (Link siehe unten).
3. Falls nicht, Prüfung ob der Eintrag des VVT im Regelwerk des WP248 mindestens in zwei Kategorien eingeordnet werden kann. Bei innovativen Technologien kann auch nur ein Eintrag ausreichend sein (Link siehe unten).
4. Falls nicht, Prüfung ob angedachte technische und organisatorische Maßnahmen für einen Eintrag des VVT eine wirksame Risikoeindämmung im Sinne der Rechenschaftspflicht nach Art. 5 DS-GVO plausibel erscheinen lassen.
5. Sollten die oben genannten Punkt 1-4 nicht zu einem voraussichtlich hohen Risiko führen, dann sehen wir (in dieser Prüfung) keine Datenschutzfolgenabschätzung als erforderlich an.

Weiterführende Links zum Thema:

- ✓ **Bayerisches Landesamt für Datenschutzaufsicht:**
Ausführliche Informationen zur DSFA, insbesondere Schwellwertanalysen
https://www.lida.bayern.de/de/thema_dsfa.html
- ✓ **Datenschutzkonferenz:**
Working Paper 248 der Datenschutzgruppe nach Artikel 29: „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt‘“
https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf
- ✓ **Datenschutzkonferenz:**
„Muss-Liste“ der Datenschutzkonferenz zum Thema DSFA
https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- ✓ **EU-Recht:**
Erwägungsgrund 75 der Datenschutzgrundverordnung
<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE#page=15>