

Aktuelle Informationen zu Corona / Covid-19 finden Sie [hier](#).

# Datenschutz-Folgenabschätzung

Die Datenschutz-Grundverordnung (DSGVO) regelt die Rahmenbedingungen für Datenschutz und Datensicherheit. Hierbei führt sie für die Verarbeitung von personenbezogenen Daten einen risikobasierten Ansatz ein. Dies bedeutet: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die DSGVO an die Anwendung, Art. 24, 32 DSGVO. Immer dann, wenn eine Datenverarbeitung für die Rechte und Freiheiten einer Person ein hohes oder ein sehr hohes Risiko zur Folge hat, hat der Verantwortliche vor deren Einführung eine sog. Datenschutz-Folgenabschätzung (DSFA) vorzunehmen und zu ermitteln, welche Folgen eine geplante Verarbeitung für den Schutz der Daten Betroffener hätte. Über das Instrumentarium der DSFA sollen Risiken beschrieben, bewertet und reduziert werden.

Lässt sich ein (sehr) hohes Risiko nicht durch angemessene technische und/oder organisatorische Maßnahmen reduzieren, ist für den Einsatz der Anwendung vorab eine Genehmigung der zuständigen Datenschutzaufsichtsbehörde einzuholen.

Eine DSFA ist zu überprüfen und anzupassen, sollten neue Risiken hinzukommen, die bereits behandelte Risiken ändern oder wesentlich erschweren. Über Prüfroutinen kann sichergestellt werden, dass eine DSFA noch aktuell ist.

## Behandlung bereits vorhandener Datenverarbeitungen

Für diese gibt es keinen Bestandsschutz, d. h. eine DSFA ist durchzuführen, wenn die Voraussetzungen hierfür vorliegen oder neue Risiken zu einer entsprechenden Wertung führen. Gestützt auf Erwägungsgrund 171 der DSGVO sehen die Leitlinien zu DSFA der Art.-29-Datenschutzgruppe (Stand: 04.10.2017)\* vor, dass eine DSFA nicht durchzuführen ist, wenn eine Datenschutzaufsicht oder ein Datenschutzbeauftragter eine Datenverarbeitung im Wege einer sog. "Vorabkontrolle" vorab geprüft hat. Derartige Prüfentscheidungen bleiben in Kraft, bis diese geändert, ersetzt oder aufgehoben sind.

## Vorgehensweise

1. Für jede Verarbeitung ist mittels einer systematischen Risikobewertung (sog. „Schwellenwertanalyse“) zu klären, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Das Ergebnis ist zu dokumentieren (z. B. bei der Beschreibung der Verarbeitung im sog. Verzeichnis von Verarbeitungstätigkeiten).
2. Für mehrere ähnliche Verarbeitungsvorgänge (umfasst alle Daten, Systeme (Hard- und Software) und Prozesse) reicht eine Abschätzung, sofern diese ein ähnlich hohes Risiko haben.
3. Vorstufe einer Risikobewertung ist eine Schutzbedarfsfeststellung der zu verarbeitenden personenbezogenen

Daten anhand der Datenarten (Kundendaten, Mitarbeiterdaten, Steuerdaten, Gesundheitsdaten etc.)

#### WEITERE HINWEISE ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG

- [Newsletter EU-Datenschutz-Grundverordnung - Nr. 14 \(PDF / 142 KB\)](#)