

Verbindliche Datenschutzvorgabe: **Durchführung von Datenschutzfolgenabschätzungen („DSFA“)**

Gesetzliche Hintergrundinformationen

Gemäß Art. 35 DS-GVO muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Erläuterung der erforderlichen Maßnahmen

Unter bestimmten Umständen muss vor Go-Live eines neuen Services oder einer Software eine umfangreiche Dokumentation der rechtlichen Prüfung, der Risiken und der Maßnahmen in Form einer sog. Datenschutz-Folgenabschätzung erstellt werden. Diese Dokumentation enthält mindestens folgende Informationen:

- Eine systematische Beschreibung der beabsichtigten Verarbeitungen sowie deren Zwecke
- Die Prüfung der Rechtmäßigkeit der Verarbeitungen
- Die legitimen Interessen des Verantwortlichen an den Verarbeitungen
- Eine Bewertung der Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen, die mit den Verarbeitungen verbunden sind
- Die beabsichtigten Abhilfemaßnahmen zur Bewältigung der dargestellten Risiken
- Falls erfolgt, die Einbindung der Betroffenen

Vorgehen und Verantwortlichkeiten

1. Der Fachbereich muss die künftige Verarbeitungstätigkeit im Verzeichnis der Verarbeitungstätigkeiten („VVT“) in der Datenschutz-Management-Software OneTrust dokumentieren (siehe auch Datenschutzvorgabe zum VVT).
2. GCO führt im VVT die Prüfung der datenschutzrechtlichen Zulässigkeit durch und bewertet, welche Risiken für die Rechte und Freiheiten der Betroffenen bestehen und ob eine DSFA erforderlich ist.
3. Sollte eine DSFA erforderlich sein, wird das OneTrust Assessment der rechtlichen Prüfung um eine vollständige DSFA erweitert und eine umfangreiche Risikobewertung durchgeführt.
4. Anschließend erfolgt eine Prüfung und Bewertung der Angaben durch den Datenschutzbeauftragten.
5. Die in OneTrust dokumentierten Risiken werden einem Vertreter des verantwortlichen Fachbereiches zur Umsetzung von risikomitigierenden Maßnahmen zugewiesen und deren Umsetzung durch das Datenschutz-Management überwacht.
6. Im Fall eines verbleibenden Risikos ist vor Go-Live abschließend durch den Fachbereichsvertreter die Freigabe der GF/GL einzuholen und ggf. vom Datenschutz-Management die Aufsichtsbehörde zur informieren.

Das Datenschutz-Management koordiniert die Durchführung der DSFA unter Beteiligung des Fachbereichs, GCO, der Informationssicherheit und des Risk-Managements sowie des DSB.

Weiterführende Informationen

Ansprechpartner: GCO; Datenschutz-Management; Informationssicherheit; DSB