

Verbindliche Datenschutzvorgabe: **Beauftragung von Auftragsverarbeitern („AV“)**

Gesetzliche Hintergrundinformationen

Erfolgt eine Verarbeitung durch einen Auftragsverarbeiter („AV“), so darf der Verantwortliche gemäß Artikel 28 DS-GVO nur mit Dienstleistern arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen („TOMs“) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt.

Erläuterung der erforderlichen Maßnahmen

Wenn personenbezogene Verarbeitungen an einen AV ausgelagert werden, muss mit dem Dienstleister begleitend zum Hauptvertrag zusätzlich eine sog. Auftragsverarbeitungs-Vereinbarung abgeschlossen werden („AV-Vereinbarung“ oder „AVV“). Diese muss u.a. folgende Informationen und Regelungen enthalten:

- Details zur Verarbeitung gem. Art. 30 DS-GVO (Verarbeitungsverzeichnis)
- Ort der Datenverarbeitung (innerhalb/außerhalb der EU bzw. EWR)
- Kontrollrechte des Auftraggebers
- Regelung zu Haftung und Vertragsstrafen sowie etwaige Unterauftragnehmer
- Angaben zur Datenschutz-Organisation inkl. Kontaktdaten des DSB
- Beschreibung der technischen & organisatorischen Maßnahmen („TOMs“) des Dienstleisters

Die Angaben aus der AVV, insbesondere die TOMs, müssen im Regelfall vor der ersten Datenübermittlung und später in regelmäßigen Abständen überprüft werden.

Diese Überprüfung erfolgt abhängig vom Umfang und Risiko der Verarbeitung durch Vorlage aussagekräftiger Zertifikate oder Unterlagen aus anderen Auditierungen bis hin zu Vor-Ort Audits durch einen sachverständigen Dritten, d.h. einem für die LP-Gruppe tätigen externen qualifizierten Audit-Dienstleister. Zur Dokumentation von Informationen zu den eingesetzten AVs sowie zur Durchführung von Dienstleister-Assessments wird die Datenschutz-Management Software OneTrust eingesetzt.

Seitens des für den Dienstleister verantwortlichen Mitarbeiters ist entsprechend auf das Vorliegen einer von beiden Parteien gegengezeichneten AVV zu achten. Erst im Anschluss an die erfolgreiche Überprüfung der TOMs dürfen dem Dienstleister dann personenbezogene Daten zur Verarbeitung überlassen oder diesem Zugriff gewährt werden.

Vorgehen und Verantwortlichkeiten

1. Der Fachbereich bzw. Mitarbeiter, der den Dienstleister einsetzen möchte, kontaktiert das Datenschutz-Management und GCO um eine AVV abzuschließen.
2. Das Datenschutz-Management unterstützt den Fachbereich bei Abstimmung des ausgefüllten AVV-Templates, Prüfung der TOMs zusammen mit Information Security und ggf. Einschaltung von GCO bei Änderungswünschen zu Standard-Vertragsklauseln. Dabei erfolgt die initiale Prüfung von Audit-Maßnahmen.
3. Das Datenschutz-Management pflegt und aktualisiert fortlaufend die Information zum AV in der Vendor-Datenbank im Datenschutz-Management-Tool OneTrust und nutzt diese zur Planung von Audit-Maßnahmen.
4. Der Fachbereich stellt sicher, dass die durch den AV durchgeführten Prozesse im Verzeichnis der Verarbeitungstätigkeiten dokumentiert sind (siehe Datenschutzvorgaben „VVT“).
5. Das Datenschutz-Management führt zusammen mit dem Fachbereich das Off-Boarding nicht weiter beauftragter AV durch, beendet AVVs und prüft Löschbestätigungen.

Weiterführende Informationen

Ansprechpartner: Datenschutz-Management (Jens Selbach); GCO; DSB
Templates: AV-Vereinbarung