Clouddienstleister und VDA / ISA TISAX®

Als Unternehmensberater im Bereich TISAX® werden unsere Berater immer wieder mit der Frage konfrontiert, in welchem Umfang und unter welchen Bedingungen die Zusammenarbeit mit Cloudanbietern möglich ist. Gerne möchten wir hier etwas Klarheit schaffen.

Brauchen alle Clouddienstleister mit denen ich zusammenarbeite eine TISAX®-Zertifizierung?

Ein entsprechendes Label ist für den Clouddienstleister ***nicht verpflichtend***, erleichtert aber die Abarbeitung der notwendigen Cloud-Kontrollfragen.

Grundsätzlich stellt die Zusammenarbeit mit Cloudanbietern **kein Hindernis dar**, sofern diesbezüglich keine anderen Aussagen und Informationen seitens des OEM existieren, auf denen sich die Zusammenarbeit begründet.

Im Anforderungskatalog VDA / ISA TISAX® ist klar geregelt in welchem Umfang und unter welchen Bedingungen in der Cloud gearbeitet werden darf.
Es gibt **keine explizite Anforderung** das eine TISAX-Zertifizierung erforderlich ist. Um sicher zu gehen sollte jedoch eine vergleichbare Zertifizierung der Cloud-Lösung - wie zum Beispiel die ISO 27001 - seitens des Anbieters vorhanden sein.

Wer sich den Anforderungskatalog VDA / ISA 5.0.3 in der aktuellen Version ansieht erkennt in der Spalte „Referenz zu anderen Standards“ jene Kontrollfragen die auf „Cloud“ abzielen. Diese sind meist mit einem „CLD“ gekennzeichnet (z.B. Referenz zu ISO 27017: CLD.14.1.1).

Die Zusammenarbeit mit fremden IT-Serviceanbietern (u. a. Cloudanbietern) regeln folgende Kontrollfragen:

Kontrollfrage 1.2.4:

Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?

Es ist wichtig, dass ein gemeinsames Verständnis der Verantwortungsaufteilung existiert und die Umsetzung aller Sicherheitsanforderungen sichergestellt wird. Bei der Nutzung von organisationsfremden IT-Dienstleistungen und IT-Diensten sind deshalb die Verantwortlichkeiten bezüglich der Umsetzung von Maßnahmen zur Informationssicherheit festzulegen und nachweisbar zu dokumentieren.

Kontrollfrage 1.3.3:

Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?

Insbesondere bei organisationsfremden IT-Diensten, die mit geringen Kosten oder kostenfrei nutzbar sind, besteht ein erhöhtes Risiko, dass die Beschaffung und Inbetriebnahme ohne geeignete Berücksichtigung der Informationssicherheitsanforderungen erfolgt und somit die Sicherheit nicht gewährleistet ist.

Kontrollfrage 5.3.3:

Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus Organisationsfremden IT-Diensten geregelt?

Um als Informationseigentümer die Hoheit über die Informationswerte zu gewährleisten, ist es erforderlich, dass im Falle einer Beendigung des IT-Dienstes die Informationswerte wieder sicher entfernt werden können bzw. bei Bedarf zurückgegeben werden.

Kontrollfrage 5.3.4:

Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?

Damit die eigenen Informationen in organisationsfremden IT-Diensten jederzeit geschützt werden und nicht durch weitere Organisationen (Mandanten) zugreifbar sind, muss eine klare Trennung zwischen den einzelnen Mandanten gewähreistet sein.

Ihre digIT 4u GmbH

Marcel Hofmann

Marcel Hofmann
Head of Consulting