Checkliste: IT-Sicherheit bei externen Dienstleistern und Lieferanten

Fragen	Ja	Nein
Wird erfasst, welche externen Dienstleister Zugriff auf IT-Systeme oder Daten haben (z. B. Softwareanbieter, Zahlungsdienstleister, Technikpartner)?	☐	☐
Wird bei neuen Dienstleistern geprüft, ob sie IT-Sicherheitsstandards einhalten?	☐	☐
Werden von Softwareanbietern oder IT-Dienstleistern Sicherheitsnachweise oder Zertifikate eingefordert (z. B. ISO 27001, Penetrationstests)?	☐	☐
Können die wichtigsten Anbieter nachweisen, dass sie regelmäßig Sicherheitsprüfungen durchführen?	☐	☐
Sind in den Dienstleisterverträgen Mindestanforderungen an die IT-Sicherheit enthalten?	☐	☐
Enthalten die Verträge Regelungen dazu, wer im Falle eines Sicherheitsvorfalls verantwortlich ist?	☐	☐
Gibt es klare Vorgaben, wie im Fall eines Datenlecks oder IT-Vorfalls zu handeln ist?	☐	☐
Haben externe Dienstleister nur Zugriff auf die Systeme oder Daten, die sie für ihre Arbeit benötigen?	☐	☐
Werden diese Zugriffsrechte regelmäßig überprüft und bei Bedarf entzogen?	☐	☐
Wird dokumentiert, wer wann auf welche Daten oder Systeme Zugriff hatte?	☐	☐
Werden größere, sicherheitskritische Software-Updates (z. B. für Türsysteme oder Kassensoftware) vorab getestet und nicht ungeprüft installiert?	☐	☐
Werden diese Sicherheitsthemen bereits heute bei der Auswahl neuer Anbieter berücksichtigt?	☐	☐