datenschutz-berater.de

44. Jahrgang

DSB 09/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz
Schriftleitung: Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Stichwort des Monats

Datenschutz im Fokus

Fragen aus der Praxis

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Anna Cardillo

Zertifikat nach ISO/IEC 27001: Hinreichende Garantie des Auftragsverarbeiters im Sinne von Art. 28 Abs. 1 DSGVO?

Der Verantwortliche soll nach Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der Betroffenen gewährleistet ist. Darum schlägt das Herz eines Verantwortlichen höher, wenn der Dienstleister ein Zertifikat nach ISO/IEC 27001 vorlegen kann, in der Regel in der Annahme, dieses bescheinige die IT-Sicherheit und damit den Schutz personenbezogener Daten. Dieser Beitrag als Auftakt einer Beitragsreihe zur ISO/IEC 27001 beleuchtet die Frage, ob die selbst unter Datenschutzberatern weit verbreitete Annahme gerechtfertigt ist.

Auswahl des Auftragsverarbeiters

Den Verantwortlichen trifft nach Art. 28 Abs. 1 DSGVO bei der Auswahl des Auftragsverarbeiters eine Prüfpflicht. Der Auftragsverarbeiter soll dem Verantwortlichen hinreichend Garantien bieten, wobei der Begriff der hinreichenden Garantien selbst nicht definiert ist. Erwägungsgrund 81 DSGVO stellt vor allem auf die Sicherheit der Verarbeitung (Art. 32 DSGVO) ab. Die vom Dienstleister angebotenen technischen und organisatorischen Maßnahmen müssen dazu geeignet sein, die Schutzziele des Art. 32 DSGVO sicherzustellen. Daneben müssen hinreichende Garantien insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen des Auftragsverarbeiters vorliegen. Der Verantwortliche hat sich bei der Prüfung daher ein möglichst umfassendes Bild zu machen. Je nach Gefährdungspotential für die Betroffenen, Umfang der Verarbeitung oder Schutzbedarf der Daten können Interviews, Fragebögen, aber natürlich auch Vor-Ort-Kontrollen geeignete Mittel zur Prüfung sein. Zertifikate, Kundenaudits des Verantwortlichen oder eigene/beauftragte Audits des Auftragsverarbeiters können für ausreichende Garantien i. S. d. Art. 28 Abs. 1 DSGVO sorgen.

Der Verantwortliche muss im Streitfall die Erfüllung der gesetzlich vorgesehenen Prüfpflicht nachweisen können. Es empfiehlt sich daher, einen Auswahlprozess zu implementieren und die Ergebnisse der Prüfung zu dokumentieren.

Genehmigte Zertifizierungsverfahren nach Art. 42 DSGVO

Art. 28 Abs. 5 DSGVO sieht die Möglichkeit vor, die Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO durch den Auftragsverarbeiter als Faktor heranzuziehen, um hinreichende Garantien i. S. d. Art. 28 Abs. 1 DSGVO nachzuweisen.

Ein nach Art. 42 und Art. 43 DSGVO i. V. m. § 39 BDSG genehmigtes Zertifizierungsverfahren gibt es noch nicht. Die Frage, ob und inwieweit ein erfolgreich durchlaufendes und nach Art. 42 und Art. 43 DSGVO i. V. m. § 39 BDSG genehmigtes Zertifizierungsverfahren eine weitere Prüfpflicht des Verantwortlichen entfallen lässt, kann daher an dieser Stelle nicht beantwortet werden. Bislang sind noch nicht einmal Zertifizierungsstellen akkreditiert. Die Aufnahme der Tätigkeit als Zertifizierungsstelle i. S. d. § 39 BDSG setzt eine Akkreditierung durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit der Befugnis erteilenden, zuständigen Datenschutz-Aufsichtsbehörde voraus. Die deutschen Aufsichtsbehörden haben sich bislang mit der DAkkS lediglich auf Standards und Anforderungen in Bezug auf künftige Zertifizierer und Zertifizierungsprogramme verständigt. Hierzu steht die Stellungnahme des Europäischen Datenschutzausschusses gemäß Art. 64 DSGVO allerdings noch aus.

Grundlage für die Aufnahme als Zertifizierungsstelle ist die DIN ISO/IEC 17065. Die Datenschutzaufsichtsbehörden haben ergänzende Anforderungen zu dieser Norm aufgestellt. Die Kapitel adressieren neben allgemeinen Themen auch Anforderungen an die Struktur, die Ressourcen, die Prozesse und an das Managementsystem der zu akkreditierenden Stelle.

Als Gegenstand der Zertifizierung im Rahmen eines Zertifizierungsprozesses sollen Datenverarbeitungsvorgänge zulässig sein, die in Produkten, Prozessen und Dienstleistungen oder mit Hilfe von (auch mehreren) Produkten und Dienstleistungen erbracht werden. Managementsysteme als Steuerung der Datenverarbeitung sind hingegen als Zertifizierungsgegenstand ausgeschlossen.

Die hohen Anforderungen an die Akkreditierung von Zertifizierungsstellen, vor allem mit Blick auf die benötigten personellen und fachlichen Ressourcen, lassen zeitnahe Akkreditierungen von Zertifizierungsstellen allerdings nicht erwarten.

Ein Zertifikat nach ISO/IEC 27001 ist mithin kein Zertifikat nach Art. 42 und Art. 43 DSGVO und befreit den Verantwortlichen nicht von seiner Prüfpflicht nach Art. 28 Abs. 1 DSGVO.

Die ISO/IEC 27001- ein Überblick

Dennoch kann die Zertifizierung eines Auftragsverarbeiters nach ISO/IEC 27001 geeignet sein, über bestimmte vorhandene Prozesse und Maßnahmen Auskunft zu geben und zur Beurteilung des Gesamtbildes vor allem in Bezug auf die in Art. 32 DSGVO geforderten Maßnahmen beitragen. Die ISO/IEC 27001 hat sich als internationaler Standard für die Informationssicherheit etabliert. Sie enthält Anforderungen für Planung, Aufbau, Betrieb und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Ein Managementsystem ist eine strategische Organisationsform, eine systematische, gezielte und geplante Herangehensweise an die Umsetzung von Unternehmenszielen (hier Sicherheitszielen).

Ein Zertifikat nach ISO/IEC 27001 attestiert dem Auftragsverarbeiter hingegen nicht die IT-Sicherheit, wenn auch von den Anforderungen der Norm IT-Systeme ebenfalls erfasst sein können.

IT-Sicherheit ist eine Teilmenge der Informationssicherheit und behandelt den Schutz von IT-Systemen. Informationssicherheit hat hingegen das Ziel, Informationen jeglicher Art (Informationen z. B. in IT-Systemen, auf Papier, oder auch nur in den Köpfen der Nutzer) zu schützen und reicht damit viel weiter als die IT-Sicherheit. Die klassischen Schutzziele der Informationssicherheit und damit des ISMS sind Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, deren Sicherstellung in Bezug auf personenbezogene Daten auch in Art. 32 DSGVO gefordert wird. Weitere Schutzziele aus dem Datenschutz, wie z. B. Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sind in der Regel von einem ISMS nicht erfasst. Über die Rechtmäßigkeit der Datenverarbeitungen trifft ein Zertifikat nach ISO/IEC 27001 ebenfalls keine Aussage.

Der Verantwortliche muss nachvollziehen können, nach welchen Kriterien das Zertifizierungsaudit erfolgte, will er das ISO-Zertifikat im Auswahlverfahren zugunsten des Auftragsverarbeiters werten. Schließlich muss er beurteilen können, ob die Einhaltung dieser Kriterien Gewähr für die Einhaltung der in Art. 28 und Art. 32 DSGVO niedergelegten Pflichten – zumindest in Teilen – bietet.

Die ISO/IEC 27001 ist Teil der sehr umfangreichen Normenreihe ISO 27000. Die Hauptnorm ist die 27001, die 27002 bis 27007 sind unterstützende Normen. Daneben gibt es branchen- und sektorspezifische Normen u. a. für den Finanz-, Telekommunikations- und Healthbereich sowie themenspezifische Standards. Beispielhaft seien die 27017/27018 für Informationssicherheit und Datenschutz in der Cloud (kein akkreditiertes Verfahren nach Art. 42 DSGVO), ISO 27031 für Business Continuity Management und ISO 27039 für Intrusion Prevention genannt.

Die zentrale Norm ISO/IEC 27001 besteht aus einem Hauptteil und einem Anhang A. Der Hauptteil besteht aus den zwingend umzusetzenden Kapiteln 4-10, der Anhang A ist in 14 Themen unterteilt und enthält insgesamt 114 Sicherheitsanforderungen (sog. Controls). Diese muss der Auftragsverarbeiter nicht alle umgesetzt haben, wenn er der Auffassung ist, dass diese für ihn nicht relevant sind. Setzt er Anforderungen nicht um, muss es dies jedoch begründen.

Abhängig von der Zertifizierungsstelle können Zertifikate nach ISO/IEC 27001 mit einer Gültigkeit von bis zu drei Jahren ausgestellt werden. Nach Ablauf der Gültigkeitsdauer ist eine Re-Zertifizierung möglich. Zusätzlich sind, abhängig von der Zertifizierungsstelle und der Gültigkeitsdauer des Zertifikates, gegebenenfalls jährliche Überwachungsaudits notwendig.

Manche Stellen vergeben Zertifikate mit ein-, zwei- oder dreijähriger Gültigkeit, verlangen aber in diesem Intervall jährliche Audits. Andere Stellen beschränken die Gültigkeit von vorneherein auf ein Jahr.

Mit dem Zertifikat nach ISO/IEC 27001 wird dem Auftragsverarbeiter bescheinigt, dass bestimmte von der ISO/IEC 27001 geforderte technische und organisatorische Maßnahmen zum Zeitpunkt eines Zertifizierungsaudits anhand von stichprobenhaft erhobenen Auditnachweisen durch den Auditor der Zertifizierungsstelle festgestellt werden konnten. Damit ist allerdings noch keine Aussagekraft für die Datenschutzrelevanz verknüpft, sie kann an dieser Stelle aber auch noch nicht per se verneint werden. Der Verantwortliche muss prüfen, ob das vorhandene ISMS und damit die getroffenen technischen und organisatorischen Maßnahmen des Dienstleisters in Bezug auf die klassischen Schutzziele der Informationssicherheit geeignet sind, die vom Verantwortlichen bereitgestellten personenbezogenen Daten angemessen zu schützen und ob sie damit den Anforderungen von Art. 28 und Art. 32 DSGVO genügen.

Geltungs- oder Anwendungsbereich

Für jedes Managementsystem, so auch für eines nach ISO/IEC 27001, muss ein Anwendungsbereich (sog. Scope) klar festlegt sein. Hier ist bereits für den Verantwortlichen Vorsicht geboten. Der Auftragsverarbeiter ist nämlich relativ frei in dem „Zuschnitt“ seines ISMS, sodass der Verantwortliche als erstes dringend prüfen sollte, ob der im Zer-

tifikat angegebene Geltungsbereich den entsprechenden Bereich des Auftragsgegenstandes umfasst.

Ein ISMS kann sich auf das gesamte Unternehmen erstrecken. Es kann aber auch nur auf Teile, einzelne Abteilungen, einzelne Geschäftsprozesse oder bestimmte Standorte beschränkt sein. Dabei kann der Auftragsverarbeiter den Anwendungsbereich frei nach eigenen Vorstellungen festlegen. Es nützt dem Verantwortlichen wenig, wenn der Auftragsverarbeiter beispielsweise ein bestimmtes Rechenzentrum an einem bestimmten Standort einer Zertifizierung unterworfen hat, die Daten des Verantwortlichen aber in einem anderen Rechenzentrum liegen. Genauso wenig hilft es dem Verantwortlichen, wenn der Auftragsverarbeiter mit IT-Services (z. B. Support) beauftragt werden soll, das ISMS sich hingegen lediglich auf die Softwareentwicklung erstreckt.

Personenbezogene Daten als schutzbedürftige Assets im Rahmen der ISO/IEC 27001

Nachdem der Anwendungsbereich festgelegt ist, ist nach ISO/IEC 27001 im Rahmen der Planung des ISMS eine initiale Risikoanalyse durchzuführen. Alle im Geltungsbereich relevanten Assets müssen zuvor inventarisiert und die Risiken für diese Assets identifiziert werden (sog. Assetmanagement). Unter Assets wird alles verstanden, was für das Unternehmen einen Wert darstellt. Die Festlegung der zu schützenden Werte und deren Schutzbedarf bildet das Fundament für ein wirksames ISMS. Alle Assets, die für den Anwendungsbereich wesentlich sind, müssen dabei betrachtet werden. Für jedes – nach eigenem Ermessen – als schützenswert festgestelltes Asset muss das Unternehmen festlegen, welche Auswirkungen ein etwaiger Verlust von Vertraulichkeit, Integrität und Verfügbarkeit hat. Je nach Risikobewertung müssen die 114 Controls aus dem Anhang A für diese Assets abgearbeitet werden.

Hat das Unternehmen personenbezogene Daten im Rahmen des Assetmanagements nicht als schützenswerte Assets im Anwendungsbereich identifiziert und dem ISMS zugrunde gelegt, so wird die initiale Risikoanalyse die personenbezogenen Daten nicht berücksichtigen. Die Maßnahmen würden in einem solchen Fall an den personenbezogenen Daten vorbei geplant.

Hat das Unternehmen personenbezogene Daten hingegen als schützenswerte Assets identifiziert und in der initialen Risikoanalyse behandelt, so kann es bestimmte Sicherheitsanforderungen aus den 114 Controls für diese Assets nach eigenem Ermessen umsetzen oder schlicht als irrelevant einordnen. Hier kann es durchaus zu einer Lücke zwischen der Erwartungshaltung des Verantwortlichen und der tatsächlichen Umsetzung der Sicherheitsanforderungen durch den Auftragsverarbeiter kommen.

Die sogenannte State of Applicabilty (SoA) ist das zentrale Dokument des ISMS nach ISO/IEC 27001. In der SoA wird dokumentiert, wie die Informationssicherheit in der Organisation umgesetzt ist. Sie enthält eine Erklärung zu allen 114 Controls aus dem Anhang A der ISO/IEC 27001. Dieses zentrale Dokument kann dem Verantwortlichen als Grundlage zur weiteren Prüfung und für weiterführende Gespräche mit dem Auftragsverarbeiter, ob und wenn ja, welche Sicherheitsanforderungen wie umgesetzt wurden, dienen.

Fazit:

Ein ISO/IEC 27001 Zertifikat ist kein Zertifikat nach Art. 28 Abs. 5 und Art. 42 DSGVO. Es trifft auch keine Aussage über die weiteren Schutzziele aus dem Datenschutz wie z. B. Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sowie über die Rechtmäßigkeit einer Datenverarbeitung. Dennoch kann es als Grundlage für eine Prüfung herangezogen und bewertet werden, um sich ein Gesamtbild vom Auftragsverarbeiter zu verschaffen. Besonderes Augenmerk sollte auf den Geltungsbereich und das Assetmanagement des Auftragsverarbeiters gelegt werden. Mindestens das Zertifikat und (noch viel wichtiger) die SoA sollte der Auftragsverarbeiter vorlegen können.

In der Praxis lässt sich leider beobachten, dass vor allem große Player als Auftragsverarbeiter der Bitte um Vorlage von weiteren Dokumenten nicht nachkommen. Selbst das Zertifikat als solches wird nicht vorgelegt. Solche Auftragsverarbeiter müssten an dieser Stelle bereits bei der Auswahl ausscheiden. Das vorbehaltlose Zur-Kenntnis-Nehmen des Zertifikats oder der bloßen Behauptung einer Zertifizierung ohne weitere Prüfung erfüllt die Prüfpflicht des Verantwortlichen nach Art. 28 Abs. 1 DSGVO jedenfalls nicht. Die Gültigkeitsdauer des Zertifikats sollte beachtet und nach deren Ablauf die Re-Zertifizierung erfragt werden.

Datenschutzberatern sei daher dringend empfohlen, sich näher mit dem Aufbau und den Regelungsinhalten der ISO Norm zu beschäftigten, um weitere Prüfungen, zum Beispiel durch gute Fragen, vornehmen zu können. Die nächsten Beiträge dieser Beitragsreihe geben einen tieferen Einblick in die Welt der ISO/IEC 27001 und Empfehlungen für weitere Prüffragen.

Autorin: **Anna Cardillo ist Rechtsanwältin bei Spirit Legal und spezialisiert auf Datenschutz- und Informationssicherheitsrecht. Sie berät Verantwortliche vor allem bei der Implementierung eines integrierten Informationssicherheits- und Datenschutzmanagements.**