datenschutz-berater.de

44. Jahrgang DSB 11/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Dr. Carlo Piltz
Bußgelder sind nicht alles Seite 261

Stichwort des Monats

Frederick Richter
Zentral oder dezentral, das ist hier die Frage … Seite 262

Datenschutz im Fokus

Guido Hansch
Whistleblowing-Richtlinie EU 2019/1937: Neue Compliance-Anforderungen für Unternehmen (Teil 2) Seite 266

Lea Stegemann und Dr. Max Grewe
Caught between a rock and a hard place? Arbeitgeber zwischen Daten- und Infektionsschutz? Seite 269

Anna Cardillo und Andreas Bethke
Der „nichtverhandelbare" Hauptteil der ISO/IEC 27001 und die Bedeutung für den Datenschutz Seite 273

Fragen aus der Praxis

Dr. Carlo Piltz und Johannes Zwerschke
Von Newslettern und Datenschutzverletzungen Seite 277

Aktuelles aus den Aufsichtsbehörden

Tilman Herbrich
EDSA: Neue Leitlinien zum Konzept der Verantwortlichkeit und Auftragsverarbeitung in der DSGVO Seite 280

Rechtsprechung

Dr. Jan-Peter Ohrtmann und Carl Christoph Möller
BGH: Auslistung wegen „Recht auf Vergessenwerden" erfordert umfassende Grundrechtsabwägung Seite 283

Dr. Alexander Golland
Immaterieller Schadensersatz für die Weiterleitung von Daten über ein berufsbezogenes soziales Netzwerk Seite 286

▪ **Nachrichten** Seite 264 ▪ **Service** Seite 290

ISSN 0170-7256

dfv Mediengruppe

Anna Cardillo und Andreas Bethke

Der „nichtverhandelbare“ Hauptteil der ISO/IEC 27001 und die Bedeutung für den Datenschutz

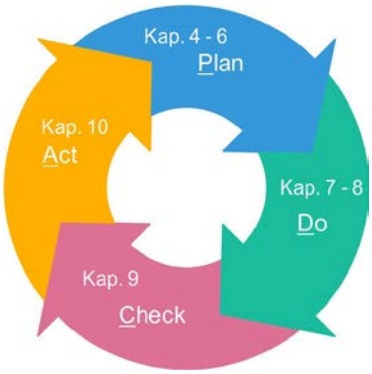
Im letzten Beitrag wurde die Frage behandelt, ob eine Zertifizierung nach ISO/IEC 27001 als hinreichende Garantie des Auftragsverarbeiters im Sinne von Art. 28 Abs. 1 DSGVO herangezogen werden kann. Wenig verwunderliches Fazit: Es kommt darauf an. Im Folgenden soll die ISO/IEC 27001 daher näher beleuchtet werden. Der zweite Teil der Beitragsreihe setzt dabei den Fokus auf die zwingend umzusetzenden Anforderungen der Kapitel 4–10 und beleuchtet die Frage, inwieweit die Umsetzungsmaßnahmen bedeutsam für den Datenschutz sein können und worauf ein Verantwortlicher bei der Überprüfung seines Auftragsverarbeiters achten sollte.

Kapitelübersicht

Die ISO/IEC 27001 besteht aus insgesamt 11 Kapiteln und einem Anhang A. Nach Einleitung, Anwendungsbereich (der Norm an sich), normative Verweisungen und Begriffsdefinitionen folgen die zwingend umzusetzenden Abschnitte. Der Aufbau folgt der sogenannten High Level Structure (HLS) der ISO-Managementsysteme gemäß ISO/IEC Directives aus 2012. Alle ISO-Managementsysteme haben im Hauptteil folgende Abschnitte:

Kap. 0	Einführung
Kap. 1	Anwendungsbereich
Kap. 2	Normative Verweise
Kap. 3	Begriffe
Kap. 4	Kontext der Organisation
Kap. 5	Führung
Kap. 6	Planung
Kap. 7	Unterstützung
Kap. 8	Betrieb
Kap. 9	Bewertung der Leistung
Kap. 10	Verbesserung

Die HLS orientiert sich ihrerseits an dem bekannten PDCA-Zyklus, auch wenn die aktuellen ISO-Normen diesen nicht mehr explizit benennen.



Die Kap. 4–10 schreiben für die Umsetzung keine konkreten Sicherheitsmaßnahmen oder Methoden vor. Hier kann ein Unternehmen weitestgehend frei wählen und gestalten. Der Verantwortliche sollte daher im Rahmen des Auswahlverfahrens mit offenen Fragen nach dem „Wie“ der Umsetzung an den Auftragsverarbeiter herantreten.

Kap. 4 Kontext der Organisation

Das Unternehmen, das ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 implementieren möchte, wird als „Organisation“ bezeichnet. Am Anfang der Implementierung steht die Analyse und Beschreibung des eigenen Umfeldes, um so ein Verständnis für die Organisation und deren Kontext zu gewinnen. Dabei sollte der Geschäftszweck oder die Geschäftstätigkeit der Organisation im Fokus stehen. Dies bedeutet, dass zunächst alle Themen im Kontext der Geschäftstätigkeit bestimmt werden, die Auswirkungen auf die Informationssicherheit haben. Dabei werden externe und interne Einflüsse betrachtet und die entsprechenden Informationen zusammengetragen. Zu den externen Einflüssen zählen beispielsweise: gesetzliche Rahmenbedingungen, finanzielle Aspekte, Technologie- (Abhängigkeiten), Lieferketten, Art und Umfang bestehender Vertragsbeziehungen zu Kunden und Partnern und vieles mehr.

In Kap. 4.2 wird die Zusammenstellung sogenannter „interessierter Parteien“ gefordert. Zentrales Thema an dieser Stelle ist, welche der genannten Parteien Einfluss auf das ISMS einer Organisation hat und welche Anforderungen sie an das ISMS stellt (konkrete Vorgaben, bestimmte Sicherheitsstufen, etc.). Diese Anforderungen können gesetzliche Vorgaben sowie vertragliche Verpflichtungen beinhalten. Bei einem Dienstleister, der maßgeblich als Auftragsverarbeiter tätig ist, sollten daher die gesetzlichen und vertraglichen Anforderungen an Auftragsverarbeitungsverhältnisse (Vertrag, Inhalt, Überprüfung, Mitwirkung, Subunternehmer etc.) bekannt sein. Häufig findet man allerdings in entsprechenden Unterlagen lediglich „DSGVO/BDSG“, ohne dass konkret der Aspekt der Auftragsverarbeitung betrachtet wurde. Demzufolge ist zu befürchten, dass die Vorgaben zur Auftragsverarbeitung auf operativer oder prozessualer Ebene nicht im

Sinne des Verantwortlichen (Auftraggebers) umgesetzt sind.

In Kapitel 4.3 wird der Anwendungsbereich des ISMS festgelegt und es werden die Grenzen abgesteckt. Die ISO/IEC 27001 selbst macht hier keine Einschränkungen, so dass sich ein ISMS z. B. auf eine Entwicklungsabteilung (nebst Support), ein ganzes Rechenzentrum oder aber auch auf ein ganzes Unternehmen erstrecken kann. Hier gilt es als Verantwortlicher bei der Prüfung eines Dienstleisters ganz genau hinzuschauen. Die zentrale Frage lautet: Erstreckt sich das (zertifizierte) ISMS auch auf den Bereich, in dem meine Daten im Auftrag verarbeitet werden?

Kap. 5 Führung

In diesem Kapitel geht es um Führung und Verpflichtung, die Informationspolitik sowie Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.

Kap. 5.1 stellt einige Aufgaben und Pflichten der obersten Leitung (Unternehmensleitung) auf. Ihre primäre Aufgabe ist die Übernahme der Verantwortung in Bezug auf Informationssicherheit. Dabei können Aufgaben an zuständige Stellen delegiert werden. Das Zuweisen von Zuständigkeiten und Aufgaben, das Unterstützen sowie die Kontrolle der Ergebnisse sind nicht delegierbar.

Neben einer Leitlinie, die Informationssicherheitspolitik und -ziele enthält, müssen Rollen, Verantwortlichkeiten und Befugnisse beschrieben werden. In einem Zertifizierungsaudit wird sich ein ISO/IEC 27001-Auditor die Leitlinie, deren Unterzeichnung durch die Unternehmensleitung und Bekanntmachung gegenüber den Mitarbeitern in der Regel nachweisen lassen. Ressourcen lassen sich durch Budgetplanungen nachweisen, die Delegation von Aufgaben durch entsprechende Stellenbeschreibungen, Protokolle, E-Mails etc.

Verantwortlichen wird nicht selten der Einwand entgegengebracht, dass Dokumente aufgrund der Vertraulichkeit nicht gezeigt, geschweige denn herausgegeben werden dürften. Aufgrund des häufig vorherrschenden wirtschaftlichen Ungleichgewichts (großer Dienstleister vs. kleiner Auftraggeber) dulden Verantwortliche eine solche Verweigerungshaltung oder haken hier gar nicht erst nach. Das Interesse eines Auftragsverarbeiters, aus wirtschaftlichen Gründen externe Einzelaudits im Auswahlverfahren oder nach Vertragsschluss zu vermeiden, ist nachvollziehbar. Eine pauschale Ablehnung der Herausgabe von schriftlichen Nachweisen ist jedoch mit Blick auf Art. 28 Abs. 1 und 3 lit. h) DSGVO nicht gerechtfertigt. Es ist zudem ein Signal dafür, dass im Rahmen der Ermittlungen des Kontexts „Auftragsverarbeitung" die externe Partei „Verantwortlicher" und die gesetzlichen/vertraglichen Rahmenbedingungen möglicherweise nicht hinreichend beleuchtet wurden. Der Auftragsverarbeiter kann zumindest auf konzeptioneller Ebene durchaus Dokumente wie das Sicherheitskonzept (einschließlich Leitlinie und Beschreibung der Organisation) an den Auftraggeber herausgeben. Einige Firmen haben erkannt, dass es durchaus ein Wettbewerbsvorteil sein kann, den Informationssicherheitsprozess zu beschreiben und dieses Konzept zu veröffentlichen, ohne dass die eigene Informationssicherheit kompromittiert würde (Beispiel AEB: https://service.aeb.de/fileadmin/public_documents/LeitlinienUndZertifikate/Leitlinie_Integriertes_Managementsystem.pdf). Über die Werthaltigkeit eines Konzepts lässt sich streiten. Es trägt jedenfalls zum Gesamtbild bei, welches sich der Auftraggeber nach dem Willen des Verordnungsgebers machen soll. Auftragsverarbeitern sei empfohlen, ein entsprechendes Dokument für interessierte Parteien wie Auftraggeber bereit zu halten. Jedenfalls ist es dringend geboten, im Vertrag über Auftragsverarbeitung gemäß Art. 28 Abs. 3 lit. h) DSGVO detaillierte Regelungen aufzunehmen, um Klarheit zu schaffen. In der frühen Phase des Auswahlverfahrens kann die Lösung für den Verantwortlichen darin liegen, sich vom ISB/DSB des Auftragsverarbeiters anhand eines Fragenkatalogs Informationen einzuholen und sich mindestens nach Leitlinie, Unterzeichnung, Bekanntmachung, Organisation Datenschutz und Informationssicherheit zu erkundigen.

Kap. 6 Planung

Das Kapitel 6 der ISO/IEC 27001 beschäftigt sich mit der Planung zur Erreichung von Informationssicherheitszielen sowie dem Umgang mit Risiken und Chancen. Hier wird der Verantwortliche im Rahmen einer Prüfung meist keinen Einblick bekommen.

Kap. 7 Unterstützung

Hierunter sind alle begleitenden Anforderungen zusammengefasst, die zur Sicherstellung der Fähigkeit und Wirksamkeit des ISMS dienen. Die Norm fordert von der Unternehmensleitung, Ressourcen (Menschen und Mittel) zur Verfügung zu stellen, die über ausreichend Kompetenzen verfügen. Ohne einen Blick in die ISO-Dokumente zu werfen, kann ein Verantwortlicher Prüffragen nach (fachlicher) Qualifikation und Schulung der Mitarbeiter eines Auftragsverarbeiters stellen. Neben der Kompetenz ist auch das Bewusstsein für die Informationssicherheit entscheidend. Jeder Mitarbeiter im Anwendungsbereich muss die Informationssicherheitspolitik kennen und sie müssen sich bewusst sein, welchen Beitrag sie selbst zur Informationssicherheit leisten und welche Folgen die Nichterfüllung von Anforderungen an das ISMS hat. Dies kann der Verantwortliche gut in einem Interview „abklopfen" oder nach entsprechenden Schulungen oder konkreten Sensibilisierungsmaßnahmen fragen.

In diesem Zusammenhang ist es auch von Bedeutung wie die interne und externe Kommunikation ausgestaltet ist.

Gemeint ist damit die Kommunikation in Bezug auf das ISMS. Es soll im Detail festgelegt werden, wer mit wem kommuniziert und kommunizieren darf, wann und wie mit welchem Inhalt die Kommunikation zu erfolgen hat. Anlass kann zum Beispiel ein Sicherheitsvorfall sein, der Kommunikationsbedarf mit Auftraggebern (Verantwortlichen), Meldestellen, Aufsichtsbehörden oder Pressestellen auslöst. Für den Verantwortlichen ist dieser Punkt von hoher Brisanz, er sollte daher überprüfen, ob die im Vertrag zur Auftragsverarbeitung aufzunehmenden Mitwirkungspflichten des Auftragsverarbeiters mit den internen Regelungen zur Kommunikation korrespondieren.

Im letzten Abschnitt des Kapitels geht es dann um die sogenannten dokumentierten Informationen. Ohne die ISO- Dokumente selbst einzusehen, kann der Verantwortliche durch gezielte Fragen nach dokumentierten Prozessabläufen schnell einen Eindruck bekommen, ob das Unternehmen die Anforderungen erfüllt. Die Organisation ist nämlich gemäß der ISO/IEC 27001 verpflichtet, dokumentierte Informationen vorzuhalten, die einerseits von der ISO/IEC 27001 selbst gefordert werden und andererseits als Nachweis für die Wirksamkeit des ISMS dienen. Ohne Auditnachweis gibt es keine Zertifizierung. Verantwortliche können zum Beispiel danach fragen, in welchem Dokument die Methodik der Risikoanalyse hinterlegt ist, wie Daten über Sicherheitsvorfälle erfasst werden, wie Schwachstellentests und Audits dokumentiert werden, wie Sensibilisierungsmaßnahmen nachgewiesen werden etc.

Kap. 8 Betrieb

Das Kapitel 8 trägt die Überschrift "Betrieb". Hier beschreibt die Organisation die operative Tätigkeit innerhalb der Grenzen des ISMS, also wie die Informationssicherheit tatsächlich gelebt wird. Dazu gehört die Planung und Steuerung bestimmter Maßnahmen, die ergriffen werden, um die Sicherheit der Informationen zu gewährleisten, Betriebsmittel zu schützen und die eigentlichen Geschäftsprozesse am Laufen zu halten. Im Kern dreht sich dabei alles um den risikobasierten Ansatz und somit um die Risikoanalyse. Aus Datenschutzsicht könnte man nun aufatmen, denn auch dort wird der risikobasierte Ansatz gefordert. Allerdings betrachtet die Risikoanalyse eines ISMS lediglich die Risiken für das Unternehmen. Die Risikoanalyse im Bereich Datenschutz betrachtet die Risiken für die Betroffenen. Die Aufnahme von Betroffenenrisiken in die Risikoanalyse eines ISMS wäre nur ein kleiner Schritt, den jedoch die wenigsten Unternehmen gehen. Die Empfehlung an den Verantwortlichen lautet daher, ganz konkret nach einer solchen Implementierung zu fragen.

Kap. 9 Bewertung der Leistung

Nachdem ein ISMS geplant und umgesetzt wurde, sieht die Norm im Kapitel 9 eine Bewertung der Leistung vor. Zunächst muss dabei festgelegt werden, was genau überwacht und gemessen wird, wie dies wann und durch wen geschieht und wie die Bewertung aussieht. Hier lohnt es sich sogenannte Key-Performance-Indicators (KPIs) zu definieren. Dazu könnten Datenschutzvorfälle oder Informationssicherheitsvorfälle, aber auch von Externen durchgeführte Penetrationstests zählen. Außerhalb des Zertifizierungsprozesses fordert die Norm zwar keine weiteren externen Audits, jedoch muss in geplanten Abständen ein internes Audit durchgeführt werden. Je nach Aufgabenbereich des Auftragsverarbeiters lohnt es sich nach entsprechenden externen Prüfungen zu fragen. So gewinnt der Verantwortliche einen Eindruck, wie wichtig das Thema "Sicherheit" für den Auftragsverarbeiter ist, auch wenn ihm der Einblick in die vertraulichen Ergebnisse verwehrt wird. Abschließend muss in Kapitel 9 der ISO/IEC 27001 noch die Managementbewertung erfolgen. Ziel dabei ist es, dass das Management (als treibende Kraft) die Eignung, Angemessenheit und Wirksamkeit des ISMS bewertet und sicherstellt.

Kap. 10 Verbesserung

Im letzten Kapitel 10, das die Überschrift "Verbesserung" trägt, geht es darum zu definieren, wie ein Unternehmen mit Nichtkonformität und Korrekturmaßnahmen umgeht. Nichtkonformitäten, die durch ein internes oder gar externes Audit festgestellt wurden, müssen bewertetet und ggf. durch Korrekturmaßnahmen behandelt werden. Diese müssen überwacht und in ihrer Wirksamkeit bewertet werden. Zuletzt verlangt die Norm noch, dass es eine fortlaufende Verbesserung des ISMS geben muss. Hier schlägt sich die Bewertung durch das Management aus dem vorigen Kapitel nieder. Auch hier wird der Verantwortliche als Externer in der Regel keine Einsicht bekommen.

Kern des ISMS: Die Risikoanalyse

Die Risikoanalyse bildet den Kern des ISMS. Dabei darf das Unternehmen sowohl die Einschätzung der abhängigen Parameter (Eintrittswahrscheinlichkeit und Schadensausmaß) als auch die Akzeptanzgrenze des Risikos selbst festlegen. Sofern ein Risiko als nicht mehr akzeptabel eingestuft wird, müssen Maßnahmen geplant und umgesetzt werden, um das Risiko zu minimieren oder bestenfalls zu eliminieren. Diese Maßnahmen können nach Bedarf gestaltet oder aus einer beliebigen Quelle ausgewählt werden. So können sich Unternehmen der Maßnahmen z. B. aus dem BSI-Grundschutz bedienen. Die Norm selbst liefert im Anhang A.5 bis A.18 Ziele und Maßnahmen, anhand derer sich das Unternehmen orientieren soll, um zu prüfen, ob sich die eigenen Maßnahmen mit den vorgegebenen Zielen und Maßnahmen decken. Nähere Ausführungen zu den Maßnahmen aus dem Anhang A der ISO/IEC 27001 werden dann in der ISO 27002 beschrieben. Die Norm sagt aber sehr deutlich, dass die Liste der Maßnahmen nicht erschöpfend ist und dass weite-

re Maßnahmenziele und Maßnahmen erforderlich sein könnten.

Fazit

Verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen und setzt er dafür Systeme ein, die im Anwendungsbereich des ISMS liegen, so sagt die Umsetzung der Anforderungen aus dem Hauptteil der ISO/IEC 27001 nichts über konkrete Sicherheitsmaßnahmen oder gar deren Angemessenheit im Hinblick auf die Risiken für die Rechte und Freiheiten der Betroffenen aus. Die Kap. 4–10 beschreiben auf der Meta-Ebene konzeptionell den Informationssicherheits-Managementprozess mit dem Ziel der kontinuierlichen Verbesserung und dienen damit (nur) mittelbar der Datensicherheit. Die Anforderungen sind zwingend umzusetzen. Die konkrete Ausgestaltung dieses Prozesses ist von der ISO-Norm nicht vorgeschrieben, jedoch korrespondieren im Anhang A bestimmte Controls mit den Anforderungen. Kennt man die Controls genauer, lassen sich daraus Prüffragen ableiten. Zu diesem Thema soll die Beitragsreihe fortgesetzt werden.

Autoren: **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.**

Andreas Bethke ist Diplom Informatiker bei B3. Neben seiner Tätigkeit als externer Datenschutz- und Informationssicherheitsbeauftragter sowie als Datenschutzauditor berät er Unternehmen bei der Implementierung von ISMS nach ISO/IEC 27001.