ISO/IEC 27001 trifft DS-GVO

Was leistet der internationale Standard für Informationssicherheit mit Blick auf die neue DS-GVO?

Für immer mehr Unternehmen ist Informationssicherheit ein zentrales Thema, das mit einem herkömmlich implementierten Qualitätsmanagementsystem nach ISO 9001 allein nicht abgedeckt werden kann. Dabei ist der Schutz wertvoller Informationen vor unbefugtem Zugriff nur ein Aspekt. Spätestens mit Anwendung der bereits in Kraft getretenen EU-Datenschutz-Grundverordnung (DS-GVO) ab 25. Mai 2018 erhält auch der Schutz personenbezogener Daten eine Dimension, die bei betroffenen Unternehmen bereits jetzt einen nicht unerheblichen Handlungsbedarf erfordern kann. Mit einem zertifizierten Informationssicherheits-Managementsystem (ISMS) gemäß ISO/IEC 27001 kann eine Reihe wesentlicher Anforderungen der DS-GVO abgedeckt werden, zumal es für diese noch kein akkreditiertes Zertifizierungsverfahren gibt.

ISO/IEC 27001 wurde aus der britischen Vorgängernorm BS 7799 entwickelt und im Jahr 2005 erstmals veröffentlicht. Mit der Revision im Jahr 2013 erhielt der Informationssicherheitsstandard als eine der ersten ISO-Normen die so genannte High Level Structure (HLS), eine gemeinsame Grundstruktur, mit der bis heute annähernd alle wichtigen ISO-Managementsystemnormen ausgestattet wurden. Den Anforderungen liegt – wie von ISO 9001:2015 bekannt – ein prozessorientierter und risikobasierter Ansatz zugrunde, was die zurzeit in der Version ISO/IEC 27001:2015 vorliegende Norm in gewissen Grenzen auch für klassische Aufgaben des Qualitätsmanagements tauglich macht. Der Standard ist Teil einer Normenfamilie, die für spezielle Branchenbedingungen eigene Versionen enthält. Im Zusammenhang mit dem IT-Sicherheitskatalog ist zurzeit vor allem ISO/IEC 27019 mit speziellen Anforderungen für Energienetzbetreiber von Bedeutung.

Unternehmen, die ihre Informationen in einer so genannten Public Cloud speichern, können bereits seit August 2014 auf das Regelwerk ISO/IEC 27018 zurückgreifen. Das Mitglied der „ISO 27000"-Normenfamilie ist speziell auf den Umgang mit Daten ausgerichtet, die nicht mehr, wie herkömmlich, auf einem lokalen Rechner gespeichert sind, sondern in einer „Rechnerwolke". Vor allem im Zusammenhang mit Auftragsdatenverarbeitung wurden hier bereits wesentliche Anforderungen der DS-GVO vorweggenommen.

„In den letzten 12 Monaten wurden zwei Drittel der deutschen Unternehmen Opfer von IT-Vorfällen."

Ergebnis einer Studie von Bitkom Research im Auftrag von F-Secure, Oktober 2017

Ein Vergleich

Mit Blick auf die neue DS-GVO kann ISO/IEC 27001 Unternehmen, die personenbezogene Daten verarbeiten, besonders auch im Zusammenhang mit dem dazugehörigen Leitfaden zur Implementierung des Managementsystems, ISO/IEC 27002, gute Dienste leisten. Dies ist vor allem darin begründet, dass mit der Erfüllung der Normanforderungen gleichzeitig auch wichtige Bereiche der EU-Verordnung abgedeckt sind. Eine Gegenüberstellung der wesentlichen Anforderungen der DS-GVO mit denen aus ISO/IEC 27001 zeigt, wo dies der Fall ist, und an welchen Stellen Ergänzungen notwendig sind.
Der Vergleich gilt aber auch in umgekehrter Richtung: Hat ein von der DS-GVO betroffenes Unternehmen alle Maßnahmen getroffen, um deren Anforderungen zu erfüllen, sollte es überlegen, ob sich der logische Schritt zu einem vollumfänglichen ISMS nach ISO/IEC 27001 zur grundlegenden Sicherung der IT und sämtlicher anderer Informationen – und vor allem auch als geeignete Managementsystemgrundlage – nicht lohnt.

Risikobetrachtung/Compliance

DS-GVO: Das Nichteinhalten der neuen DS-GVO-Anforderungen kann mit sehr hohen Geldstrafen geahndet werden (Art. 83). Die konkrete Summe orientiert sich am weltweiten Jahresumsatz der jeweiligen Muttergesellschaft (4 Prozent) und kann bis zu 20 Mio. Euro betragen.

Wichtig bei der Risikobetrachtung im Rahmen der Datenschutz-Folgenabschätzung (Art. 35) ist die Betrachtung aus Sicht des Betroffenen. Diese steht der Betrachtung aus Sicht der Informationssicherheit konträr gegenüber. Hinweise oder Vorgaben zur Methodik gibt die DS-GVO nicht. Hier kann man sich den Regelungen von ISO/IEC 27005, dem BSI Standard 100-3 oder ISO 31000 bedienen. Achten Sie dabei immer auf den Kontext (aus Sicht der betroffenen Person).
ISO/IEC 27001: Das Regelwerk verlangt die Risikoabschätzung u. a. der Werte (A.8.1), was angesichts der durch die neue DS-GVO entstehenden finanziellen Risiken auch den Umgang mit personenbezogenen Daten umfasst. Das Thema

Mitglied im bitkom

Compliance wird insofern abgedeckt, als ISO/IEC 27001 verlangt, dass in Frage kommende gesetzliche bzw. vertragliche Anforderungen dokumentiert werden, deren Einhaltung gewährleistet ist und die Folgen bei Nichteinhaltung ermittelt werden.

Klassifizierung von Daten

DS-GVO: Gefordert wird, dass der Schutz personenbezogener Daten im Zuge ihrer Verarbeitung gewährleistet wird (Art. 5). Die Bedeutung personenbezogener Daten (nach Kategorien) ergibt sich dabei aus den jeweiligen Artikeln der Verordnung.
ISO/IEC 27001: Der internationale Standard fordert, dass Unternehmen erhaltene Daten gemäß ihrer Bedeutung schützen müssen (A.8.2).

Meldepflicht bei Datenpannen

DS-GVO: Wird einem Unternehmen eine Datenpanne bekannt, muss es diese laut DS-GVO innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde melden (Art. 33).
ISO/IEC 27001: Die Norm fordert einen Prozess, der den Umgang mit Vorfällen regelt, der die Informationssicherheit betrifft. Auch hier müssen diese Vorfälle schnellstmöglich gemeldet werden (A.16.1.2).

Zusammenarbeit mit Behörden

DS-GVO: Die Verordnung verlangt von Unternehmen die Zusammenarbeit mit den zuständigen Behörden (Art. 31).
ISO/IEC 27001: Auch die Norm für Informationssicherheit spricht von geeigneten Kontakten zu relevanten Behörden (A.6.1.3), was in der Praxis auf das Gleiche hinausläuft.

Management von organisationseigenen Werten

DS-GVO: Unternehmen müssen hier Folgendes nachvollziehen können (Art. 5):

- die Art der personenbezogenen Daten
- wie diese in den Besitz des Unternehmens gekommen sind
- wo sie gespeichert sind
- wer die Zugriffsrechte hat

ISO/IEC 27001: Hier wird gefordert, die organisationseigenen Werte zu bestimmen und wer für deren Schutz verantwortlich ist. Die Werte müssen aufgelistet, ihr Eigentümer ermittelt werden. Außerdem bedarf es konkreter Regeln für den Umgang mit diesen Werten und was mit ihnen nach ihrem Lebenszyklus geschehen soll (A.8.1).

„Eingebauter" Datenschutz

DS-GVO: Die Verordnung fordert den Schutz personenbezogener Daten, und zwar nach dem „Stand der Technik" (Art. 25 und § 71 BDSGneu).
ISO/IEC 27001: Die Norm verpflichtet ihre Anwender, die Sicherheit der Informationen schon bei der Entwicklung der verwendeten Systeme zu berücksichtigen und für den gesamten Lebenszyklus umzusetzen (A.14.1).

Lieferantenbeziehungen

DS-GVO: Kontrollen und Beschränkungen mit Lieferanten wie z. B. Internet-/Cloud-Anbieter oder externe Rechenzentren müssen nach der DS-GVO vertraglich festgehalten werden (Art. 28).
ISO/IEC 27001: Die Norm fordert analog dazu, die für die Lieferanten zugänglichen Unternehmenswerte zu schützen und die Erbringung der Dienstleistung auf Einhaltung der notwendigen Sicherheitsanforderungen zu überwachen (A.15.1).

Dokumentation

DS-GVO: Der in einem Unternehmen gemäß DS-GVO Verantwortliche muss u. a. Folgendes dokumentieren (Art. 30):

- zu welchem Zweck die Daten gesammelt und verarbeitet werden
- welche „Kategorien" von betroffenen Personen bzw. personenbezogenen Daten vorhanden sind

ISO/IEC 27001: Der Umfang der bzw. die Pflicht zur Dokumentation in Bezug auf einen Prozess orientiert sich in ISO/IEC 27001 daran, wie komplex der Prozess ist, und mit welchen anderen Prozessen er in Wechselwirkung steht (Kap. 7.5).

Delta zwischen ISO/IEC 27001 und DS-GVO

Grundsätzlich kann der Anwendungsbereich eines ISMS nach ISO/IEC 27001 von Unternehmen frei abgesteckt werden, was bedeutet, dass der Umgang mit personenbezogenen Daten ggf. gar nicht oder nur teilweise abgedeckt wird. Die DS-GVO enthält hingegen einige Anforderungen, die mit Blick auf ein ISMS gemäß ISO/IEC 27001 nicht relevant sind. Dazu gehört die Notwendigkeit, gemäß den Anforderungen der DS-GVO einen Datenschutzbeauftragten zu benennen (Art. 37) und weitere DS-GVO-spezifische Anforderungen an den Umgang mit bzw. die Korrektheit von personenbezogenen Daten, die unabhängig von einem ISMS erfüllt werden müssen. Darunter fällt beispielsweise die Sicherstellung, dass Betroffene jederzeit Auskunft zu ihren Daten erhalten können (Art. 15) und das Recht der Betroffenen auf Berichtigung ihrer Daten (Art. 16) bzw. auf deren (unverzügliche) Löschung (Art. 17).

Allgemeine Hinweise

Eine Zertifizierung nach ISO/IEC 27001 kann dazu beitragen, im Falle eines Datenschutzverstoßes das Bußgeld zu mindern (Art. 83 lit. c und ErwG 150 DS-GVO).

Im Wesentlichen unterstützt die Norm ISO/IEC 27001 bei der Umsetzung der Anforderungen des Art. 32 DS-GVO (Sicherheit der Verarbeitung).

Matthias Mühlhause
DQS-Auditor

Sebastian Harrand
DQS-Auditor

informationssicherheit@dqs.de