COMPLIANCE UND DIGITALISIERUNG

Die Digitalisierung stellt für Unternehmen, Behörden und Institutionen eine der aktuell größten Compliance-Herausforderung dar. Die procilon Schriftreihe betrachtet unterschiedliche Aspekte dieses Wandels und gibt praxistaugliche Handlungsempfehlungen.

Datenschutz TOM

Hagen Albus
Andreas Liefeith

procilon GROUP

Inhaltsverzeichnis

Über Compliance

Der übergeordnete, englische Begriff Compliance lässt sich in seiner Bedeutung nicht wörtlich in die deutsche Sprache übersetzen. Insgesamt steht er für die Einhaltung von gesetzlichen Bestimmungen, regulatorischer und selbst gesetzter Standards sowie ethischer Regeln. Eine generelle gesetzliche Regelung für Compliance besteht nicht. Wesentliche Anforderungen lassen sich aber aus der deutschen Gesetzgebung und in zunehmendem Maß aus Verordnungen der Europäischen Kommission für den Binnenmarkt ableiten.

Damit gilt der Grundsatz Compliance als Ganzes zu betrachten. Gerade dies hilft Geschäfts- und Verwaltungsprozesse so zu gestalten, dass Risiken bei der Digitalisierung minimiert werden.

Nur durch die Einbettung von Compliance-Maßnahmen in die tägliche Arbeit der Anwender entsteht so auch wirtschaftliche Nachhaltigkeit. Der Schutz von Informationen und Betriebsgeheimnissen im digitalen Zeitalter wird damit akzeptierter Bestandteil eines Ganzen und hilft Compliance-Anforderungen zu erfüllen.

Compliance-Herausforderung Datenschutz

Nicht nur, aber vor allem im Zusammenhang mit dem Datenschutz wurde die Begrifflichkeit „technisch organisatorische Maßnahmen“ - kurz TOM - eingeführt.

Schon im BDSG der alten Fassung (a.F.) wurde in § 9 auf Maßnahmen zum Schutz personenbezogener Daten verwiesen. In der aktuell gültigen DSGVO wird das Thema TOM in Art. 32 und BDSG (neu) im §64 ausführlich behandelt. Erfreulicherweise ist über den Verlauf der Zeit festzustellen, dass in der generellen Begrifflichkeit und der Systematik eine deutliche Annäherung zwischen Datenschutz und Informationssicherheit stattgefunden hat. Dennoch können die Gesetzestexte nicht alle Fragestellungen beantworten, die erforderlich sind, Compliance für den Datenschutz herzustellen. Beispielhaft seien hier die Formulierung „Stand der Technik“ und Unterschiede bei der Risikobewertung genannt.

TOM nach Bundesdatenschutzgesetz

Zur Veranschaulichung wird im Folgenden wörtlich aus dem BDSG zitiert und in tabellarischer Form allgemeinverständliche Ergänzungen formuliert:

§ 64 Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.

Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

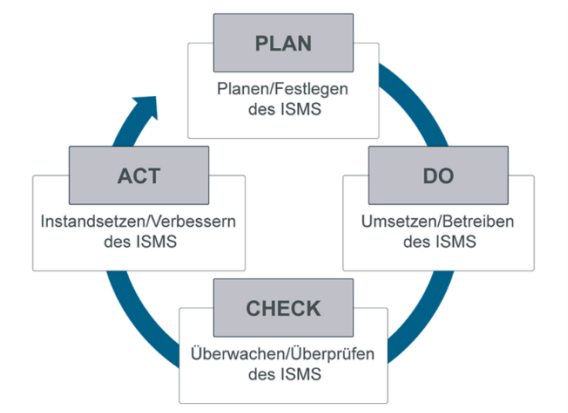
Gesetzestext	Was ist gemeint	Was ist zu tun (TOM)	procilon Lösung
Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)	Welche baulichen Maßnahmen gibt es? Wer darf in sichere Bereiche? Wie wird das überprüft?	Begehung mit IT-Sicherheitsexperten, Nutzung von Identitäts- und Zugriffs-Management zur Zutrittskontrolle	IT-Sicherheits-Beratung, proNEXT Security Manager
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)	Welche Datenträger (Festplatten, USB-Stick, CD, DVD, Band) werden verwendet? Wer darf damit arbeiten?	Bestandsaufnahme, Identitäts- und Zugriffs-Management, Verschlüsselung, Lese- und Schreibschutz, Manipulationsschutz durch Signatur	IT-Sicherheits-Beratung, proNEXT Security Manager
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)	Wer darf wann und wie mit personen-bezogenen Daten arbeiten? Wie erfolgt die Speicherung? Wer hat Zugriff?	Nachvollziehbarkeit durch automatisiertes Login, Integritätsschutz für Log-Dateien durch Signatur, Erarbeitung eines Löschkonzeptes .	IT-Sicherheits-Beratung, proNEXT Security Manager proGOV

Gesetzestext	Was ist gemeint	Was ist zu tun (TOM)	procilon Lösung
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)	Wer darf wann welche Daten wohin übertragen?	Identitäts- und Zugriffs-Management, Verschlüsselung bei der Datenübertragung, Richtlinie zur Informationskategorisierung und -übertragung	proNEXT Security Manager, proGOV, proTECTr
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)	Wer darf wann welche Daten einsehen und/oder bearbeiten?	Rollenbezogene Definition der Zugriffsberechtigungen, Identitäts- und Zugriffs-Management	proNEXT Security Manager
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)	Wer hat wann welche Daten wohin übertragen?	Protokollierung und Archivierung (z.B. E-Mail-Archivierung), Richtlinie zur Informationskategorisierung und -übertragung	proGOV
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)	Wer hat wann welche Daten eingegeben und/oder bearbeitet?	Nachvollziehbarkeit durch automatisiertes Login, Integritätsschutz für Log-Dateien durch Signatur	IT-Sicherheits-Beratung proGOV

Gesetzestext	Was ist gemeint	Was ist zu tun (TOM)	procilon Lösung
Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. (Transportkontrolle)	Wer hat wann welche Daten übermittelt?	Schutz der Daten durch Verschlüsselung und Signatur. Schreib-/Leseschutz bei Datenträgern	proGOV, proNEXT, proTECTr
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)	Was ist im Notfall zu tun?	Backup-Strategie und Notfallkonzept erarbeiten, Recovery-Test	IT-Sicherheits-Beratung
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)	Wie kann man Notfällen vorbeugen?	Monitoring-Tool mit automatisierten Benachrichtigungen. Vorbeugende Wartung.	IT-Sicherheits-Beratung
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)	Wie kann man Notfällen vorbeugen?	Geeignete Infrastruktur auswählen, Backup-Strategie entwickeln und Integritätsschutz durch Signaturen	IT-Sicherheitsberatung, proGOV
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)	Was muss beachtet werden, wenn die Daten außer Haus gehen?	Vertragliche Vereinbarung mit Auftragsnehmern, die TOM dort müssen im Minimum den eigenen TOM entsprechen.	IT-Sicherheitsberatung, Datenschutzberatung
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)	Wie kann man Notfällen vorbeugen?	Geeignete Infrastruktur schaffen, BackUp-Strategie entwickeln, Recovery-Test, Perimeterschutz	IT-Sicherheitsberatung
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)	Wer darf wann welche Daten einsehen und/oder bearbeiten?	Identitäts- und Zugriffs-Management, ggf. Mandantensysteme implementieren	IT-Sicherheitsberatung

Informationssicherheit und Datenschutz

In einer zunehmend digitalen Welt, liegt die Konvergenz von Informationssicherheit und Datenschutz auf der Hand. Auch die DSGVO basiert auf einem Risikomanagement zur Ableitung geeigneter TOM. Die geforderte zyklische Überprüfung des Datenschutzkonzeptes und der ergriffenen Maßnahmen entspricht dem PDCA-Zyklus in Management-Systemen, die einen kontinuierlichen Verbesserungsprozess beinhalten (siehe ISO-Normen). Schlussfolgernd kann man also die Aktivitäten rund um die Datenschutz-Compliance auch als Datenschutz-Management-System (DSMS) bezeichnen.



PDCA-Zyklus im ISMS

Datenschutz-Management-System (DSMS)

Auch finden sich in der Datenschutzgrundverordnung die klassischen Schutzziele der Informationssicherheit wieder

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**
- **Authentizität**

Zusätzlich führt die DSGVO den Begriff der Belastbarkeit hinsichtlich verwendeter Systeme und Dienste ein. Da dies im Weiteren nicht genauer beschrieben ist, gilt es die Interpretation dieses Begriffes in der Praxis genau zu beobachten.

Der DSMS-Zyklus

Schutzbedarf personenbezogener Daten

Generell kann man bei der Schutzbedarfsfeststellung von praxiserprobten Vorgehensmodellen der Informationssicherheit profitieren. Der Fokus liegt natürlich an dieser Stelle auf den personenbezogenen Daten. Für diese wird man eine Einstufung in die Kategorien „normal“, „hoch“ oder „sehr hoch“ treffen müssen, denn letztendlich leiten sich daraus später die TOM ab.

Risikobewertung

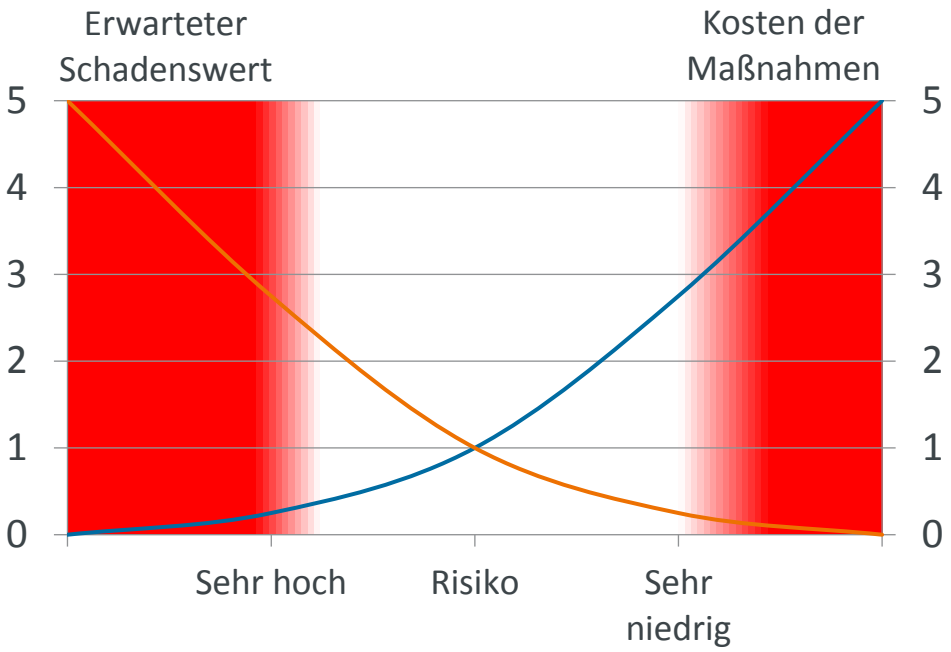
Auch für die Risikobewertung finden sich Analogien in der Informationssicherheit. Allerdings sind bei der Bewertung der Eintrittswahrscheinlichkeit im Zusammenhang mit dem Datenschutz wesentliche Unterschiede zu beachten.

Die Informationssicherheit betrachtet aus der Sicht des Unternehmens relevante Informationswerte. Der Datenschutz umfasst zusätzlich die Rechte Dritter, welche zu wahren sind. Neben der Schwere des Risikos für die Rechte und Freiheit natürlicher Personen, rücken die Risiken für betroffene Personen in den Mittelpunkt. Betroffene Personen können auch externe (z.B. Kunden, Lieferanten, Partner, Patienten, etc.) sein.

Technische und organisatorische Maßnahmen

Erwartet man an dieser Stellen genaue Handlungsempfehlungen, wird man erst einmal auf zwei Begriffe stoßen, die dies verhindern. In einem Satz zusammengefasst ist von „geeigneten“ Maßnahmen nach „Stand der Technik“ die Rede. Kritiker sehen hier zu viele Schlupflöcher. Auf der anderen Seite ist nachvollziehbar, dass der Gesetzgeber keine technischen Maßnahmen in eine Verordnung schreibt, die ggf. bei Inkrafttreten überholt sind.

Für die Festlegung geeigneter Maßnahmen sind die bereits durchgeführte Risikoanalyse und vor allem die Ermittlung des Schutzbedarfs, die elementare Grundlage. Generell sollte man zur Bestimmung der „Eignung“ einen risikooptimierten Ansatz wählen.



Zum „Stand der Technik“ hat sich inzwischen eine unter Federführung des IT-Sicherheits-Verbandes TeleTrusT entstandene Publikation bewährt. Diese wird zyklisch aktualisiert und procilon ist daran beteiligt.

Nach Betrachtung der unterschiedlichen Aspekte entsteht letztendlich ein Maßnahmenkatalog, der im Wesentlichen folgende Aspekte enthält:

- **technische Maßnahmen zur physischen Sicherheit (Zäune, Schlösser, bauliche Maßnahmen)**
- **technische Maßnahmen durch Hardware**
- **technische Maßnahmen durch Software**
- **organisatorische Maßnahmen (Mitarbeiterschulungen, Arbeitsanweisungen, Besuchermanagement)**

Nachweis der Konformität

Hier treffen wir auf die grundlegende Absicht dieses Dokumentes. Es geht letztendlich um die Einhaltung von Compliance im Datenschutz. Also den Vergleich zwischen Soll- und Istzustand. Und genau hier tritt ein ähnliches Problem wie bei dem TOM auf, denn ein eindeutiger, prüfbarer Istzustand ist bisher nicht definiert. Zwar zeichnen sich auch hier einige Parallelen zur Informationssicherheit ab, aber eine objektive Zertifizierungsmethode existiert nicht.

Das Standard-Datenschutzmodell

Als beachtenswert und zur weiteren Beobachtung empfohlen ist die Initiative der Datenschutzbehörden des Bundes und der Länder. Hier entsteht mit dem Standard-Datenschutzmodell (SDM) eine Vorgehensweise, mit der „die Übereinstimmung der gesetzlichen Anforderungen im Umgang mit personenbezogenen Daten und der entsprechenden Umsetzung dieser Vorgaben systematisch überprüfbar gemacht wird.“ Dies kann aber nur dann ein wertiges Instrument sein, wenn es, wie die DSGVO, zu einem europaweiten Standard erhoben wird.

Die Methode orientiert sich dabei an zentralen Gewährleistungszielen, wie etwa Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz etc., die über technische und organisatorische Funktionen und Schutzmaßnahmen umgesetzt werden. Das SDM soll zum einen für die Arbeit der Datenschutzbehörden einen einheitlichen, transparenten und nachvollziehbaren Rahmen bilden und zum andern Organisationen und Unternehmen dabei unterstützen, entsprechende Verfahren, die die personenbezogene Datenverarbeitung betreffen, datenschutzgerecht einzurichten und zu betreiben. Damit soll das Modell zukünftig sowohl für die Datenschutzaufsicht, im Bereich der privaten Wirtschaft, als auch im Bereich der öffentlichen Verwaltung einen wesentlichen Beitrag leisten, um einen an Grundrechten orientierten Datenschutz durchzusetzen.

Die Autoren

Hagen Albus

Geschäftsführer der jurcons GbR

Hagen Albus wurde 1964 in Treuenbrietzen geboren und studierte von 1986 bis 1990 an der Universität in Leipzig Jura. Sein Referendariat führte er in der Zeit von 1990 bis 1993 am Oberlandesgericht Bamberg durch. Im Jahr 1993 wurde er zur Anwaltschaft zugelassen und verfügt seit 1997 über den Titel des Fachanwaltes für Arbeitsrecht.

Seit 2006 ist Herr Albus als Mediator (TÜV-CERT) tätig und seit 2014 als Datenschutzbeauftragter TÜV-zertifiziert. Im Rahmen seiner Tätigkeit hat Herr Albus in verschiedenen ISMS Einführungsprojekten, vornehmlich bei Energieversorgern, Schulungen/Einführungen zum Thema Datenschutz, ISMS und Compliance gehalten.

Andreas Liefeith

Leiter Marketing, procilon GROUP

Geboren 1961, schloss Herr Liefeith 1986 sein Studium an der Technischen Universität Dresden als Diplomingenieur für Elektrotechnik ab. Von 1986-1990 war er im VEB Uhrenwerk Ruhla tätig. Von 1990 bis 2012 war Herr Liefeith Mitarbeiter der IBM Deutschland GmbH. Anfangs in der Niederlassung Erfurt und später in Leipzig.

Seit dem Jahr 2012 verantwortet er das strategische Marketing der procilon Unternehmensgruppe.

Technologie für Informationssicherheit und Datenschutz

www.**procilon.de**

procilon GROUP GmbH
Leipziger Straße 110 04425 Taucha

Kontakt:

+49 34298 4878-31 | anfrage@procilon.de