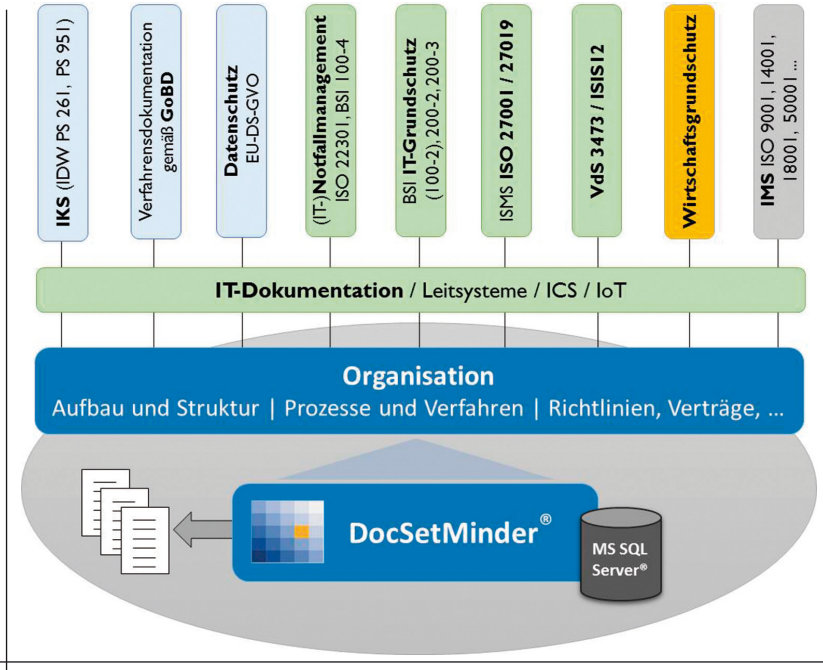
Compliance Management Software für Datenschutz, Informationssicherheit und Notfallmanagement

EU-DS-GVO mit DocSetMinder umsetzen

Viele Organisationen befassen sich zurzeit sehr intensiv mit der Umsetzung der EU-DS-GVO. Eine gezielte Betrachtung und Nutzung der Gemeinsamkeiten mit bereits etablierten oder geplanten Managementsystemen, wie z. B. ISMS, kann den nicht unerheblichen Planungs- und Implementierungsaufwand der EU-DS-GVO signifikant reduzieren.

Von Krzysztof Paschke, GRC Partner GmbH

Die EU-DS-GVO beinhaltet umfassende und detaillierte Vorgaben zu den Auskunftspflichten gegenüber von Datenverarbeitungen betroffenen Personen. Primär soll eine hohe Transparenz bei der Datenerhebung und -verarbeitung erreicht werden. Für die geforderte Transparenz und die grundsätzliche Rechenschaftspflicht der verantwortlichen Stelle ist eine aktuelle und lückenlose Dokumentation der Verarbeitungstätigkeiten notwendig. Eine fehlende oder mangelhafte Dokumentation kann mit einem Bußgeld geahndet werden. Bedingt durch die Komplexität der EU-DS-GVO und die zahlreichen Schnittmengen zum ISMS empfiehlt sich eine ganzheitliche Betrachtung der beiden Themen in einem Integrierten Managementsystem (IMS) wie DocSetMinder. Anstatt die Umsetzung von Informationssicherheit und Datenschutz einzeln zu planen und mit unterschiedlichen Tools zu realisieren, ist eine globale Sicht von enormem Vorteil. Um die Anforderungen von EU-DS-GVO und Informationssicherheitsstandards effizient und vollständig umzusetzen und aktuell zu halten, stehen den involvierten Mitarbeitern in DocSetMinder entsprechende Module und standardisierte Maßnahmenkataloge zur Verfügung.



Aufbau des Integrierten Managementsystems DocSetMinder

Dokumentation der Verarbeitungstätigkeiten

Die genaue Kenntnis der Organisation ist eine elementare Voraussetzung für die Dokumentation der Verarbeitungstätigkeiten und die Planung der technischen und organisatorischen Sicherheitsmaßnahmen. Das Modul „Organisation" stellt die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation im erforderlichen Detaillierungsgrad bereit. Erfasst werden können sämtliche Organisationseinheiten (z. B. Bereiche und Abteilungen), Geschäftsprozesse und Verfahren, ebenso wie die Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL-V.3-Struktur zur Verfügung. Das Modul enthält auch ein effizientes Richtlinienmanagement zur Verwaltung aller notwendigen Leit- und Richtlinien (EU-DS-GVO, ISMS, QM etc.). Im Vertragsmanagement werden sämtliche Sachverhalte zur Auftragsdatenverarbeitung (Auftraggeber und -nehmer) erfasst und verwaltet.

Beteiligte Anwendungen und IT-Systeme

Ein weiterer Baustein in der Umsetzung der EU-DS-GVO ist die Dokumentation des IT-Verbundes. Das Modul „IT-Dokumentation" erlaubt eine systematische Dokumentation der IT-Infrastruktur: Anwendungen und Dienste, Server-Systeme, Arbeitsplätze, Peripheriegeräte, aktive und passive Netzwerkkomponenten sowie Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt die logischen Zusammenhängte zwischen Geschäftsprozessen, Anwendungen, Serversystemen und Speicherorten für die entstehenden Informationen (Daten) dar und stellt gleichermaßen relevante, dokumentierte Sachverhalte für die Planung, Umsetzung und Aufrechterhaltung von EU-DS-GVO, ISMS und Notfallmanagementsystem bereit. Somit werden Redundanzen vermieden und Aktualisierungen vereinfacht. Die beiden Module „Organisation" und „IT-Dokumentation" bilden jederzeit transparent und nachvollziehbar die Verarbeitung personenbezogener Daten ab.

Risikoanalyse

Die verantwortliche Stelle ist verpflichtet, die Verarbeitung personenbezogener Daten durch Gestaltung der Prozesse, IT-Systeme und geeignete Maßnahmen zu schützen. Eine Risikoanalyse liefert wichtige Erkenntnisse für die Planung und Umsetzung von technischen und organisatorischen Maßnahmen. Für die Durchführung der Risikoidentifikation, -analyse, -bewertung und -behandlung steht in DocSetMinder eine Risikoanalyse gemäß ISO 31000 zur Verfügung. Von der ISO 31000 sind weitere Risikoanalysemethoden gemäß ISO/IEC 27005 und BSI-Standard 200-3 abgeleitet worden. Die Identifikation der Risiken kann unter Einbeziehung der BSI-Gefährdungskataloge (G0-G5) oder des BSI-G0-Kataloges (IT-Grundschutz-Kompendium) mit seinen elementaren Gefährdungen erfolgen. Die Gefährdungskataloge können um benutzerdefinierte Gefährdungen erweitert werden. Ein weiterer Faktor bei der Identifikation der Risiken sind die Schwachstellen. Sie werden individuell in der Organisation identifiziert und dokumentiert oder aus externen Quellen (z. B. Greenbone) in den Schwachstellenkatalog importiert. Die Risikobewertung definiert sich als Produkt aus Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) und wird mithilfe einer 4 x 4-dimensionierten Matrix durchgeführt. Die Dimension der Matrix kann individuell angepasst werden. Im weiteren Schritt wird die negative Beeinträchtigung der einzelnen Schutz- oder Gewährleistungsziele durch das festgestellte Risiko betrachtet. Im ISMS gemäß ISO/IEC 27001 oder BSI 200-3 handelt es sich dabei um Vertraulichkeit, Integrität und Verfügbarkeit. Sollte bei der Umsetzung der EU-DS-GVO das Standard-Datenschutzmodell (SDM) (Datenschutzbehörden des Bundes und der Länder) berücksichtigt werden, können in der Risikobewertung weitere Gewährleistungsziele (u. a. Belastbarkeit, Authentizität, Nichtverkettung etc.) betrachtet werden. Mit einer gut geplanten Risikoanalyse können EU-DS-GVO, ISMS, Notfallmanagement und weitere Normen in der Organisation gleichzeitig effizient behandelt werden. Ähnliches gilt auch für eine Reihe von technisch-organisatorischen Maßnahmen, die gleichermaßen für EU-DS-GVO und ISMS gelten können. Als Beispiel können hier die Zutritts-, Zugangs- und Eingabekontrolle dienen.

Modul „EU-DS-GVO"

Das DocSetMinder-Modul „EU-DS-GVO" bildet die EU-Datenschutz-Grundverordnung vollständig, detailliert und ohne Einschränkungen ab. Es bietet den verantwortlichen Mitarbeitern einen effektiven und effizienten Weg zur Planung, Einführung, Umsetzung und Überprüfung des neuen europäischen Datenschutzes. Interessierten Organisationen steht mit DocSetMinder eine leistungsfähige und intuitiv bedienbare Softwarelösung für die Umsetzung der Anforderungen der EU-DS-GVO und des BDSG-neu mit vertretbarem Aufwand zur Verfügung. Die DocSetMinder-Reporting-Services liefern Auskunft über den aktuellen Umsetzungsstatus der Maßnahmen und erinnern an deren regelmäßige Überprüfung. Die gesamte EU-DS-GVO-Dokumentation kann dem Auditor in Form von Word-Dokumenten zur Verfügung gestellt werden. Alternativ kann man die Sachverhalte auch direkt am System prüfen.

Modul „VdS 10010"

Das DocSetMinder-Modul „VdS 10010" bildet die EU-DS-GVO kompakt und übersichtlich ab und adressiert speziell kleine und mittlere Organisationen. Die Struktur und Dokumentvorlagen im Modul sind von den VdS-Richtlinien abgeleitet. Durch den kombinierten Einsatz der Module „VdS 10010" und „VdS 3473" sind KMUs bestens gewappnet für die Planung, Umsetzung und Aufrechterhaltung von Informationssicherheit und Datenschutz.

Fazit

DocSetMinder bildet die anerkannten Standards der Informationssicherheit wie auch den Datenschutz vollständig ab. Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung der umgesetzten Standards überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet allen beteiligten Mitarbeitern und Verantwortlichen einen enormen Mehrwert durch die Aktualität der Dokumentation und eine signifikante Zeitersparnis bei der Vorbereitung interner und externer Audits. DocSetMinder ist Best Practice – und ihre Organisation ist jederzeit „Ready for Audit". ■