2. AUSGABE 2020

EBNER STOLZ

novus

INFORMATIONSTECHNOLOGIE

COBIT statt COVID

Mehr Finanzen.
Mehr Anforderungen.
Mehr SWIFT.

Wegfall des Privacy-Shields – weitere Vorgehensweise

„COBIT statt COVID" – Prozessuale Neuorientierung?

Das Jahr 2020 wird uns allen noch lange in Erinnerung bleiben. Aus IT-Sicht hat die Covid-19 Pandemie die gesamte Unternehmenswelt – unabhängig von der Branche – in das digitale Zeitalter katapultiert. Speziell der flächendeckende, sehr kurzfristig konzipierte Einsatz von Softwaresystemen hat zu erheblichen Prozessveränderungen geführt und zum Teil im Laufe des Jahres zu einer prozessualen Neuorientierung beigetragen. Schließlich führte Covid-19 zwangsläufig dazu, bestehende Prozesse auf dem Prüfstand zu stellen, zu hinterfragen und an die Situation anzupassen. Man befand sich somit fast ganzjährig in einer Art Notfall.

Von besonderer Bedeutung im nächsten Jahr werden die regulatorischen Anpassungen und Änderungen im IT-Finance-Umfeld sein. Dazu gehört das ab 2021 verpflichtend durchzuführende SWIFT Community Assessment, aber auch die BAIT und die MaRisk, die sich aktuell in der Konsultation befinden.

Vor dem Hintergrund, dass der Privacy-Shield-Beschluss der EU-Kommission im Sommer 2020 für ungültig erklärt wurde, stellt sich nun (abermals) die Frage, wie personenbezogene Daten aus Europa in die USA datenschutzrechtlich unbedenklich übermittelt werden können. Wir stellen eine Vorgehensweise vor.

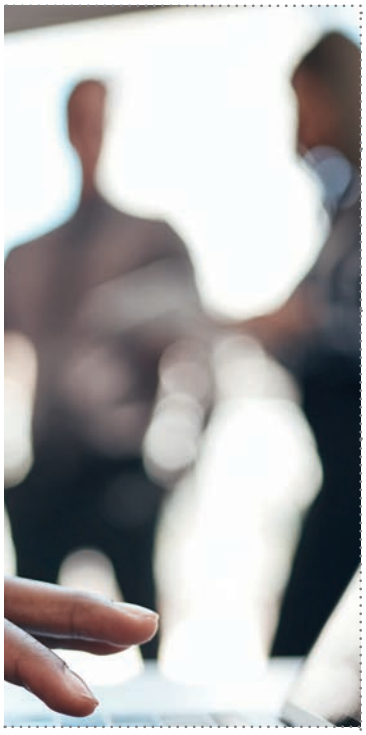
Das im Oktober veröffentlichte Patientendaten-Schutz-Gesetz hat – auch wenn man dies nicht vermuten mag – massive Auswirkungen im Informationssicherheitsumfeld von Krankenhäusern. Diese stellen wir Ihnen in dieser Ausgabe des novus IT gerne vor. Darüber hinaus beginnen wir mit einer neuen Reihe zum Thema „Migration/Umstieg auf SAP S/4HANA" und beleuchten in diesen sowie künftigen novi FAQs, die von Ihnen an den Geschäftsbereich IT-Revision herangetragen wurden. Die Beitragsauswahl wird bunt gemischt sein – betroffen sind zumeist Themen, welche nicht in den Standard-Regelwerken zur Migration beschrieben werden.

Der Geschäftsbereich IT-Revision möchte sich bei all seinen Freunden und Geschäftspartnern in diesem schwierigen Jahr für ein kooperatives, produktives und gutes Miteinander, für das weiterhin entgegengebrachte Vertrauen und die Treue sowie die angenehme Zusammenarbeit im zurückliegenden Jahr bedanken.

Bleiben Sie, Ihre Familien und Angehörigen gesund und lassen Sie uns gestärkt in 2021 gehen!

Der Geschäftsbereich IT-Revision wünscht Ihnen viel Freude bei der Lektüre und steht Ihnen bei Rückfragen natürlich gerne zur Verfügung.

Ihr GBIT



COBIT statt COVID

Die Corona-Pandemie hat Unternehmensprozesse nachhaltig verändert. Zum einen mussten innerhalb kürzester Zeit digitalisierte Strukturen geschaffen werden, zum anderen durften Aspekte, wie Cybersecurity und IT-Compliance, nicht verloren gehen. Kann z. B. ein Unternehmen kritischer Infrastruktur (KRITIS) seine Firewall-Systeme für Mitarbeiter im Home-Office öffnen? Wird das Gesamtrisiko durch fehlende Mitarbeiter oder fehlende Schutzmaßnahmen erhöht? Wie auch immer die Entscheidung ausfällt, eine strukturierte Auseinandersetzung mit IT-Compliance und IT-Governance ist zwingend erforderlich: COBIT statt COVID.

Eine der größten Herausforderungen für Unternehmen in den letzten Jahren bestand im wachsenden Druck durch die Digitalisierung. Geschäftsmodelle müssen angepasst, Prozesse überarbeitet und auch immer mehr Anforderungen müssen erfüllt werden.

Durch die Corona-Pandemie haben die Unternehmen mit zahlreichen Unbekannten zu kämpfen, die ihre Planungssicherheit zusätzlich sehr stark einschränken. Es gibt kein Patentrezept für Unternehmen, um diese Herausforderung zu bewältigen. Doch so bedrückend die weltweite Corona-Lage auch sein mag, einen positiven Nebeneffekt brachte sie mit sich: Digitale Defizite wurden deutlich und die Pandemie erhöhte den Druck, diese auch schnellstmöglich zu beheben. Von Home-Office über Home-Schooling, bis hin zu digitalen Hausarztterminen – in den letzten Monaten haben wir das alles miterlebt. Doch während Mitarbeiter mancher Unternehmen von einem Tag auf den anderen problemlos ins Home-Office umziehen konnten, mussten einige auch weiterhin vor Ort im Büro arbeiten, da dort noch regalweise die Papierordner gelagert werden oder auch schlichtweg die Softwarelösungen für digitale Zusammenarbeit noch immer fehlen. Die Krise zwingt die Unternehmen weltweit, den öffentlichen Dienst und sogar die Ärzte, endlich umzudenken – wir beobachten quasi eine Zwangsdigitalisierung.

Für die Herausforderungen, die sich durch die Digitalisierung stellen, gibt es auch nicht „die" eine Lösung. COBIT liefert allerdings ein Rahmenkonzept für Governance und Management der Unternehmens-IT und damit einen Leitfaden, den wir uns bei der Begegnung mit dem Coronavirus nur wünschen würden.

COBIT5

COBIT steht für Control Objectives for Information and Related Technology, deren erste Version bereits im Jahr 1966 veröffentlicht wurde. Die Intention der ISACA (Information Systems Audit and Control Association) bestand damals darin, ein Werkzeug für die IT-Prüfung zu entwickeln. Mittlerweile existiert COBIT in der Version 5 und auch der Anwendungsbereich hat sich erweitert. COBIT5 umfasst heute zahlreiche anerkannte Frameworks und Standards, wie bspw. Val IT und ISO-Standards. Es dient nicht mehr nur als Werkzeug für Auditoren, sondern vielmehr als Framework, mit dem die Anforderungen, die eine moderne IT an Unternehmen stellt, erfüllt werden können. COBIT5 definiert fünf Prinzipien für die Governance und das Management der Unternehmens-IT.

COBIT5 hat sich zu einem internationalen Standard für IT-General-Controls entwickelt. Die COBIT5- Prinzipien sind dabei:

1. Erfüllung der Anforderungen der Anspruchsgruppen
2. Abdeckung des gesamten Unternehmens
3. Anwendung eines integrierten Rahmenwerks
4. Ermöglichung eines ganzheitlichen Ansatzes
5. Unterscheidung zwischen Governance und Management

Erfüllung der Anforderungen der Anspruchsgruppen

Unternehmen sind zahlreichen Interessensgruppen ausgesetzt, deren Ziele häufig unterschiedlich sind. Mitunter bestehen sogar Zielkonflikte. Die Governance soll dafür sorgen, dass alle Anforderungen berücksichtigt und bewertet werden. Aus diesen Anforderungen werden mithilfe der COBIT5-Zielkaskade Unternehmensziele, IT-bezogene Ziele und sogenannte Enabler-Ziele abgeleitet. Dies funktioniert in einem Top-Down-Ansatz. Die folgenden Enabler-Kategorien beschreiben interne Ressourcen, mithilfe derer die Ziele erreicht werden sollen:

1. Prinzipien, Richtlinien und Rahmenwerke
2. Prozesse
3. Organisationsstrukturen
4. Kultur, Ethik und Verhalten
5. Information
6. Services, Infrastruktur und Anwendungen
7. Mitarbeiter, Fähigkeiten und Kompetenzen

Abdeckung des gesamten Unternehmens

Für COBIT sind nicht nur IT-Prozesse relevant, vielmehr wird das gesamte Unternehmen betrachtet: Sowohl alle internen als auch alle externen Prozesse werden adressiert. Dabei erfolgt eine Integration der IT-Governance in die Unternehmens-Governance.

Anwendung eines integrierten Rahmenwerks

COBIT5 integriert bestehende Standards und ermöglicht so die Schaffung eines einheitlichen Rahmenwerks. Bereits in der Vergangenheit wurden von der ISACA viele Rahmenwerke entwickelt, um Unternehmen in der Umsetzung zu unterstützen. Durch COBIT5 werden etablierte Standards, wie bspw. Val IT und Risk IT, in einem Framework vereint.

Hierbei wird unterschieden zwischen der Governance- und der Management-Domäne. Es werden im Rahmen des COBIT5-Prozessmodells insgesamt 37 Prozesse definiert, die in den folgenden Domänen gruppiert sind:

- **Governance-Domäne**
  Evaluieren
  Vorgeben
  Überwachen

- **Management-Domäne**
  Anpassen, Planen und Organisieren
  Aufbauen, Beschaffen und Implementieren
  Bereitstellen, Betreiben und Unterstützen
  Überwachen, Evaluieren und Beurteilen

Ermöglichung eines ganzheitlichen Ansatzes

Die Enabler-Kategorien stehen in einem direkten Zusammenhang und beeinflussen sich gegenseitig. Einzeln oder auch in Kombination sorgen sie dafür, dass die IT-Ziele des Unternehmens erreicht werden können. Durch die Erfassung interner als auch externer Anspruchsgruppen wird ein ganzheitlicher Ansatz ermöglicht.

Trennung von Governance und Management

IT-Governance und IT-Management werden in der Praxis häufig in ähnlichen Zusammenhängen verwendet. Da sich die Aufgabenbereiche jedoch stark unterscheiden und auch für COBIT5 eine klare Trennung notwendig ist, ist die Unterscheidung wichtig.

Die IT-Governance gehört zur Unternehmensführung. Der Hauptfokus liegt darauf, dass die IT die gesetzten Unternehmensziele bestmöglich unterstützt.

Das IT-Management ist dagegen eher nach innen gerichtet und planungsorientiert. Im IT-Management stehen Fragestellungen, wie die Auslastung der Systeme und die Kosten der IT, auf der Tagesordnung.

Bei COBIT wird die Unterscheidung bereits beim dritten Prinzip durch die zwei verwendeten Domänen deutlich. Beide Bereiche erfordern verschiedene Organisationsstrukturen und verfolgen unterschiedliche Zwecke, daher werden sie von COBIT5 differenziert adressiert. Trotzdem bestehen Schnittstellen zwischen den Bereichen, die zu berücksichtigen sind.

COBIT5 – Prozessbefähigungsmodell

Die Grundlage für das Prozessbefähigungsmodell bildet der Standard ISO/IEC 15504, der sich mit der Bewertung von Unternehmensprozessen befasst. So sollen im ersten Schritt verbesserungswürdige Prozesse aus den Bereichen Management und Governance identifiziert werden, um sie anschließend in die entsprechende Kategorie einzuordnen. Das Modell besteht aus fünf Stufen. Stufe 0 bezeichnet dabei einen unvollständigen Prozess – Stufe 5 kennzeichnet einen bereits optimierten Prozess. Für die Zuordnung zu der entsprechenden Stufe sind Ergebnisse, Praktiken sowie Arbeitsprodukte maßgeblich.

COBIT5 – Implementierungsleitfaden

COBIT ist ein Rahmenwerk, das individuell an das jeweilige Unternehmen angepasst werden muss. Die ISACA stellt hierzu einen Implementierungsleitfaden zur Verfügung, um Unternehmen bei der Einführung zu unterstützen und um gängige Fehler zu vermeiden. Entscheidende Punkte, die bei der Implementierung berücksichtigt werden müssen, sind bspw. das Erkennen typischer Schwachstellen und Auslöserereignisse sowie die Schaffung einer geeigneten Implementierungsumgebung. Experten aus dem Bereich IT-Servicemanagement werden sich in diesem Leitfaden schnell zurechtfinden, da derselbe Grundgedanke bereits im ITIL-Umfeld (IT Infrastructure Library) verwendet wird.

COBIT5 – Anwendung

Auf den ersten Blick könnte man meinen, die Einführung von COBIT5 wäre nur relevant für große Unternehmen. Jedoch sind die Anforderungen an die Unternehmens-IT bei allen Unternehmen unabhängig von ihrer Größe sehr ähnlich. Bei kleinen Unternehmen werden die Prozesse nicht ganz im selben Ausmaß ausgestaltet sein wie bei größeren Unternehmen. Häufig werden aber gerade bei kleineren Unternehmen im Rahmen der Einführung von COBIT Schwachstellen und Verbesserungspotenziale entdeckt. Daher sollte die Einführung nicht alleine von der Unternehmensgröße abhängig gemacht werden.

Einführung von COBIT5: Mehrwert oder nur mehr Arbeit?

Es lässt sich nicht leugnen; mit der Einführung von COBIT5 kommt auf die IT-Abteilungen zunächst eine Menge Arbeit zu. Trotzdem ist die Implementierung nahezu allen Unternehmen zu empfehlen. IT-Abteilungen haben durch COBIT5 die Chance, ihre IT selbst auf den Prüfstand zu stellen, ganz nach dem Motto: Die Schwachstellen, die wir selbst finden, können wir beheben bevor sie ein Prüfer entdeckt.

Update Kassensicherungsverordnung: Nicht-Beanstandungsregelung in fast allen Bundesländern

In den letzten Wochen und Monaten gab es hinsichtlich der aktuellen Entwicklung bei der Kassensicherungsverordnung bzw. der Nicht-Beanstandungsregelung wenig Bewegung. Dies ist sicherlich auch auf die aktuelle Pandemiesituation zurückzuführen. Mit Ausnahme des Bundeslandes Bremen haben in den Sommermonaten alle anderen 15 Bundesländer unter bestimmten Voraussetzungen eine Verlängerung der Nichtbeanstandungsregelung bis zum 31.3.2021 gewährt.

Die Voraussetzungen waren in den meisten Fällen die folgenden:

- Nachweisliche Bestellung der TSE bei einem Kassenfachhändler, einem Kassenhersteller oder entsprechenden Dienstleister bis zum 30.9.2020

oder

- Einbau einer Cloud-basierten Lösung, welche jedoch noch nicht verfügbar bzw. zertifiziert ist.

Eine gesonderte Beantragung einer solchen Fristverlängerung war bei den meisten Bundesländern explizit ausgeschlossen. Hierzu hat das Bayrische Finanzministerium ein Schreiben veröffentlicht, welches zwar anerkennt, dass eine Bewilligung des zuständigen Finanzamt gemäß §158 AO erfolgen sollte, jedoch durch die klaren Vorgaben der Nichtbeanstandungsregelung, eine einheitliche Voraussetzung statuiert wurde, bei deren Vorliegen die Bewilligung befristet zu erteilen ist bzw. als erteilt gilt.

Sofern Unternehmen nun einen Antrag stellen, müsste dieser Antrag bei Vorliegen dieser Voraussetzungen stets von der Finanzverwaltung positiv beschieden werden. Da jedoch aufgrund der Nichtbeanstandungsregelung bereits eine Fristverlängerung als erteilt gilt, sollte besser von einer Antragsstellung abgesehen werden.

Sollten Sie als Unternehmen zum jetzigen Zeitpunkt noch auf der Suche nach einer (alternativen) zertifizierten TSE-Lösung sein, so liefert das BSI unter dem folgenden Link eine Übersicht der aktuell zertifizierten technischen Sicherungseinheiten:

https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifizierteProdukte/Technische_Sicherheitseinrichtungen/TSE_node.html

Besteht bei Ihnen weiterhin Informationsbedarf hinsichtlich der grundlegenden Fragestellungen und Notwendigkeiten rund um das Thema Kassensicherungsverordnung, TSE und Verfahrensdokumentation, finden Sie in den vorausgegangen Ausgaben unseres Novus IT (Ausgaben I/2020, I/2019 und II/2018 weitere Informationen). Zudem gibt es von offizieller Seite des BSI einen umfangreichen Fragen-Antwort-Katalog, welcher für eine erste Hilfestellung nützlich sein kann:

https://www.bundesfinanzministerium.de/Content/DE/FAQ/2020-02-18-steuergerechtigkeit-belegpflicht.html

Jederzeit freuen wir uns aber auch, Ihnen für einen direkten Austausch Ihrer Fragestellungen zur Verfügung zu stehen.

Mehr Finanzen. Mehr Anforderungen. Mehr SWIFT.

Das „Society for Worldwide Interbank Financial Telecommunication" (kurz: SWIFT)-Netzwerk gilt als insgesamt gut abgesichert. Sicherheitsvorfälle in der Vergangenheit, wie der Bangladesch Bank Hack oder der Angriff auf die Indian Union Bank haben jedoch gezeigt, wie durch das gezielte Ausnutzen von vereinzelten Schwachstellen in der Sicherheitsarchitektur der Nutzer, Schäden in mehrstelliger Millionenhöhe verursacht werden können. Auswirkungen eines solchen Angriffs betreffen in einem Netzwerk wie SWIFT nicht nur einen einzelnen Nutzer, sondern zuletzt auch die ganze Community.

Auf der Grundlage der Erfahrungswerte aus den negativen Ereignissen der nahen Vergangenheit und einer generell gestiegenen Bedrohungslage, wurde im Jahr 2016 das SWIFT Customer Security Program (kurz CSP) entwickelt und veröffentlicht. Die Zielsetzung des CSP besteht insb. darin, den Mitgliedern des SWIFT-Netzwerks Mindestanforderungen und Umsetzungshinweise zur Absicherung ihrer lokalen SWIFT-Infrastrukturen an die Hand zu geben. Hierbei soll der Schutz der Community, neben der Implementierung von technischen Maßnahmen, nicht zuletzt auch durch einen aktiven Informationsaustausch zwischen den Netzwerkmitgliedern und Awareness-Maßnahmen erhöht werden.

Hinweis: Was ist das SWIFT-Netzwerk?
SWIFT wurde im Jahr 1973 mit dem Ziel gegründet, einen einheitlichen und sicheren Nachrichtendienst für Zahlungsdienste zu schaffen. Mittlerweile hat SWIFT über 11.000 Mitglieder in über 200 Ländern und ist das Rückgrat für den internationalen Zahlungsverkehr.

Überblick über das Rahmenwerk

Das Rahmenwerk des CSP bildet eine grundlegende Sicherheitsleitlinie sowie von dieser abgeleitete, konkretisierende Anforderungen in Form des Customer Security Controls Framework (kurz CSCF). Das CSCF besteht aus verpflichtend umzusetzenden (mandatory) Kontrollen und empfohlenen (advisory) Kontrollen, ergänzt um detaillierte Implementierungshinweise. Jährlich erweitert SWIFT sein Framework um zusätzliche Kontrollanforderungen und wandelt gleichzeitig empfohlene Kontrollen in Pflichtkontrollen um. Entsprechende Kontrollen werden im CSCF vorgemerkt. Es ist also durchaus sinnvoll, auch freiwillige Kontrollen bereits frühzeitig zu implementieren.

Die Ziele und Inhalte der Kontrollen des CSCF adressieren im Wesentlichen folgende Themenfelder:

- Sicherheit der IT-Infrastruktur
- Überwachung der IT-Infrastruktur
- Risikofaktor Mensch
- Benutzerberechtigungsmanagement
- Identifikation und Schließung von Schwachstellen

Die Anzahl und Art der umzusetzenden Kontrollen ist abhängig vom jeweils vorzufindenden Architekturtypen. Hier kann grundsätzlich zwischen Architekturtyp A und dem Architekturtyp B unterschieden werden. Diese übergeordneten Architekturtypen können dabei wie folgt umschrieben werden:

Architekturtyp A – bezeichnet einen Architekturtypen, bei welchem alle oder zumindest ein Großteil der für die Kommunikation mit SWIFT nötigen Komponenten in der eigenen IT-Umgebung betrieben werden.

Architekturtyp B – bezeichnet einen Architekturtypen, bei welchem alle für die Kommunikation mit SWIFT nötigen Komponenten an Dritte ausgelagert sind und mit dem SWIFT-Netzwerk nur über eine vom Dienstleister zur Verfügung gestellte Benutzeroberfläche kommuniziert wird.

Diese Architekturtypen legen hierbei nicht nur den umzusetzenden Kontrollumfang, sondern auch den einzubeziehenden Scope (SWIFT-Komponenten) fest.

2019	2020	2021
Freiwilliges Self-Assessment – CSF 2019.3	Self-Assessment – CSCF 2019.3	Pflicht Self-Assessment – CSCF 2021

Warum das CSCF jetzt besonders wichtig ist

Seit dem Jahr 2017 können Mitglieder ein freiwilliges Self-Assessment, basierend auf dem aktuellen CSCF durchführen und bei SWIFT einreichen. Der freiwillige Self-Assessment-Prozess sollte ursprünglich 2020 enden und durch das sogenannte SWIFT Community Assessment, basierend auf dem CSCF 2020 ersetzt werden.

Aufgrund der Covid-19 Pandemie wurde diese Frist um das Jahr 2021 verlängert. Für das Jahr 2020 kann nun ein letztes Mal ein freiwilliges Self-Assessment basierend auf CSCF 2019.3 erfolgen. Im Jahr 2021 muss dann das sog. SWIFT Community Assessment, basierend auf dem CSCF 2021, verpflichtend durchgeführt werden.

Sollte das Community Assessment nicht oder unzureichend durchgeführt werden, können ggf. negative Konsequenzen drohen. Zum einen werden bei einer mangelhaften oder nicht erfolgten Durchführung des Assessments die Ergebnisse einsehbar für die gesamte Community auf der Plattform Know your customer – Security Attestation (KYC-SA) veröffentlicht. Zum anderen behält sich SWIFT die Meldung der Verstöße bei den nationalen oder internationalen Aufsichtsbehörden vor.

Hinweis: Die KYC (Know your customer) Online-Plattform wird von SWIFT für seine Mitglieder bereitgestellt, um die Ergebnisse aus den durchgeführten Assessments zu melden. Zudem besteht über die Plattform die Möglichkeit, die Ergebnisse der Assessments von anderen SWIFT-Mitgliedern einzusehen. Eine Einsichtnahme ist nur dann möglich, wenn zuvor eine Freigabe durch das jeweilige SWIFT-Mitglied erfolgt ist.

Umsetzung vom SWIFT Community Assessment

Um die Umsetzung des Swift Community Assessment möglichst effektiv zu gestalten, empfehlen wir, strukturiert in einem Mehrphasenansatz vorzugehen. Diese Phasen können hierbei wie folgt gewählt werden:

Phase 1: Architekturtyp bestimmen

Bei der Bestimmung des Architekturtyps gilt es, den im Unternehmen verwendeten Architekturtyp zu bestimmen und hierauf aufbauend die relevanten CSCF Kontrollen zu identifizieren. Es ist zudem dringend notwendig, die verantwortlichen Mitarbeiter für die betroffenen IT-Systeme und Prozesse zu identifizieren.

Phase 2: Pre-Assessment

In einem Pre-Assessment werden in Form eines „Dry Run" bestehende Schwachstellen in der Anforderungsumsetzung identifiziert. Um Synergien zu nutzen, ist zu empfehlen, mögliche Schnittmengen mit bereits umgesetzten Anforderungsnormen (wie bspw. ISO 27001) zu betrachten. Das Ergebnis des Pre-Assessment sollte ein konkreter Maßnahmenplan für die Schließung identifizierter Umsetzungslücken (Schwachstellen) sein.

Phase 3: Umsetzungsphase

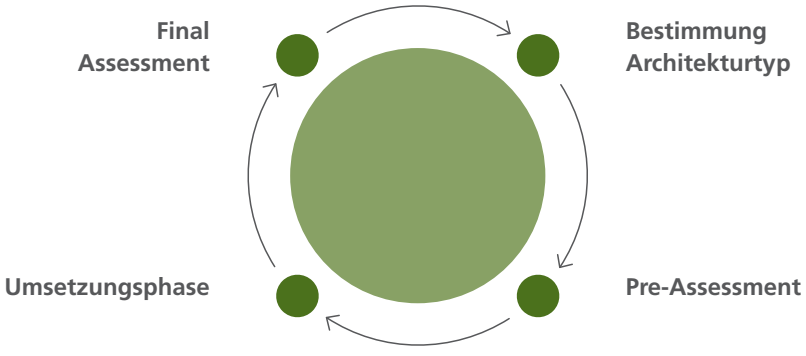
Für die Umsetzung des Maßnahmenplans aus Phase 2, sollte zunächst eine realistische, zeitliche Planung erfolgen. Die Detailtiefe des CSCF ist hierbei nicht zu unterschätzen! Zudem ist es ratsam, die IT-System- und prozessverantwortlichen Mitarbeiter, die von der Maßnahmenumsetzung direkt und indirekt betroffen sind, frühzeitig mit einzubeziehen. Als Folge der Maßnahmenumsetzung kann ggf. ein Bedarf für die Anpassung der schriftlich fixierten Ordnung (SfO) des Unternehmens sowie für die Schulung von Mitarbeitern entstehen. Wir empfehlen dringend, bei der Umsetzung von Maßnahmen, die angemessene Dokumentation von Kontrollnachweisen sicherzustellen.

Phase 4: Finales Assessment

Das finale Assessment kann intern durch die Second- oder Thirdline der Organisation oder durch einen qualifizierten externen Dienstleister erfolgen. Das Assessment ist im vorgegebenen CSCF Framework zu dokumentieren. Zudem muss eine fristgerechte Einreichung über die SWIFT-Plattform KYC-SA (muss bis 31.12. des jeweiligen Jahres erfolgen) sichergestellt werden. Ggf. identifizierte Schwachstellen sollten gemäß PDCA-Cycle in einem nächsten Schritt behoben werden.

Fazit

Mit dem Customer Security Control Framework (CSCF), als Teil des Customer Security Program, hat SWIFT ein eigenständiges Rahmenwerk geschaffen, um die Sicherheit jedes einzelnen Nutzers und damit auch der gesamten Community zu erhöhen. Hierbei enthält das CSCF sehr konkrete Anforderungen und Umsetzungshilfen, die in Bezug auf den Umfang und Detailgrad nicht unterschätzt werden sollten. Ab dem Jahr 2021 wird die Bestätigung der Konformität mit dem CSCF durch jeden Nutzer in Form eines internen bzw. externen Assessments verpflichtend sein.



Wegfall des Privacy-Shields – weitere Vorgehensweise

Mit Urteil vom 16.7.2020 (Rechtssache C-311/18, Facebook Ireland/Schrems II) wurde der Privacy-Shield-Beschluss der Kommission (2016/1250), auf dessen Grundlage bislang personenbezogene Daten aus Europa in die USA übermittelt wurden, durch den Europäischen Gerichtshof (EuGH) für ungültig erklärt. Die Entscheidung betrifft zahlreiche Unternehmen, die sich bei einem Datentransfer von personenbezogenen Daten in die USA auf das Privacy-Shield gestützt haben.

Hintergrund des Urteils

Dem Urteil lag ein Rechtstreit zwischen dem österreichischen Juristen Maximilian Schrems und Facebook zu Grunde. Initialer Streitgegenstand war der unzureichende Schutz der personenbezogenen Daten von EU-Bürgern nach Übermittlung seitens der Facebook Tochtergesellschaft in Irland an den Mutterkonzern in den USA. Schrems beantragte deshalb bei der irischen Datenschutzbehörde, die Datenübermittlungen zwischen den beiden Unternehmen auszusetzen. Facebook hingegen führte an, in bestimmten Fällen verpflichtet zu sein, die personenbezogenen Daten den amerikanischen Behörden zugänglich zu machen.

Für die Betroffenen ist dieser Datentransfer nicht transparent; ein Vorgehen gegen den Datentransfer oder dessen Einschränkung ist für die Betroffenen nur bedingt umsetzbar. Bereits im Oktober 2015 hatte der EuGH die damalige Grundlage zum Datentransfer zwischen der EU und den USA, das Safe-Harbour-Abkommen, gekippt, da nach Ansicht des EuGH kein angemessenes Datenschutzniveau gewährleistet werden konnte.

Auch das daraufhin entwickelte „Privacy-Shield" zwischen den USA und der Europäischen Union wurde nun aufgrund einer erneuten Klage vom EuGH im Juli 2020 für ungültig erklärt. Hingegen bestätigte der EuGH die grundsätzliche Wirksamkeit der Standardvertragsklauseln, stellte aber hohe Anforderungen an ihre Nutzung im Einzelfall. Ein bloßer Vertragsschluss reiche hierfür nicht aus.

Sind Standardvertragsklauseln die Lösung?

Bei der Prüfung der Standardvertragsklauseln gelangte der EuGH zu dem Ergebnis, dass diese grundsätzlich wirksam sind. Sie enthielten Mechanismen, die in der Praxis gewährleisteten, dass das in der EU verlangte Datenschutzniveau prinzipiell eingehalten würde. Somit können Standardvertragsklauseln zwar herangezogen werden, bedürfen aber einer Einzelfallbetrachtung und sind im Hinblick auf den jeweiligen konkreten Sachverhalt und das Schutzniveau der übertragenen Daten individuell auszugestalten.

Wir empfehlen jedem Datenexporteur, alle Sachverhalte, in denen personenbezogene Daten in ein Drittland übermittelt werden, aufgrund der geänderten Rahmenbedingungen nochmals zu prüfen und zu bewerten. Hierbei ist der Fokus zu legen auf:

- den Übertragungsweg der Daten,
- Menge, Art und Umfang der Speicherung der Daten,
- Maßnahmen zur Absicherung der beiden vorgenannten Punkte und
- die Prüfung von Alternativen (z. B. Dienstleister, bei denen kein Datentransfer in ein Drittland notwendig ist).

Ergibt sich aus der Bewertung, dass das Schutzniveau für die übertragenen Daten nicht mit den europäischen Standards vergleichbar ist, müssen sowohl der Datenexporteur als auch der Datenimporteur zusätzliche und für den jeweiligen Sachverhalt geeignete technische und organisatorische Maßnahmen zur Risikoreduktion festlegen bzw. umsetzen (z. B. Verschlüsselungsmechanismen oder Anonymisierungsverfahren), bis ein angemessenes Schutzniveau sichergestellt ist. Kann dies nicht gewährleistet werden, können die personenbezogenen Daten nicht auf Basis der Standardvertragsklauseln übertragen werden.

Eine erneute Prüfung, Bewertung und ggf. Ergänzung von technischen, organisatorischen oder rechtlichen Maßnahmen ist ebenfalls für die verbindlichen internen Datenschutzvorschriften (engl. Binding Corporate Rules, kurz „BCR") zu empfehlen.

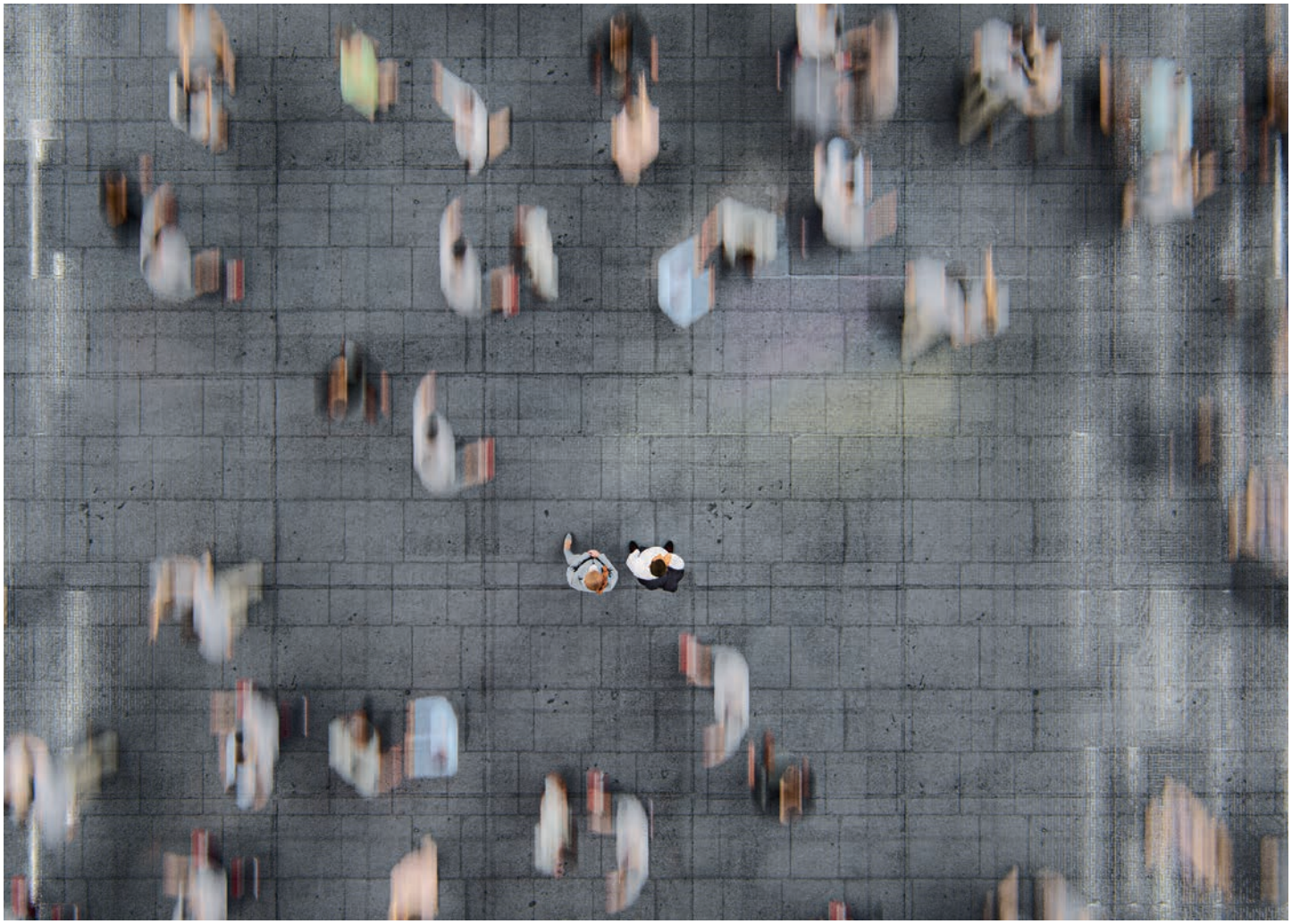
Inzwischen liegen erste Stellungnahmen der deutschen Aufsichtsbehörden zum Urteil des EuGH vor. Die konkretisierenden Ausführungen und Anforderungen der jeweiligen Landesdatenschutzaufsicht sind leider nicht deckungsgleich. Demnach sind die Ausführungen des jeweiligen Bundeslandes in die Bewertung des Datentransfers mit einzubeziehen.

Was bedeutet die Entscheidung für die Praxis?

Folgende Schritte bei der Bewertung sowie der Identifikation und Ausgestaltung risikomindernder Maßnahmen können ergänzend angewandt werden:

1. **Analyse des Datenverkehrs**
   Falls noch nicht geschehen, sollten Unternehmen den Datenverkehr in die USA analysieren und dokumentieren. Dies inkludiert auch den Datenaustausch zwischen einzelnen Konzerngesellschaften.

2. **Prüfung der Software bzw. Dienstleister**
   Anwendungen und Dienstleister sollten aufgrund der geänderten Rahmenbedingungen im Hinblick auf eine Datenweitergabe von personenbezogenen Daten in Drittländer neu beurteilt werden. Bestätigt sich der Datenverkehr, so sollte dieser umfassend analysiert und Maßnahmen zur Risikoreduktion identifiziert sowie umgesetzt bzw. vertraglich festgehalten werden.



3. Auftragsverarbeiter kontaktieren und EU-Server bevorzugen

Viele Anbieter, wie z. B. Amazon Web Services (AWS) oder Microsoft ermöglichen, dass Daten auf EU-Servern gespeichert werden können. Falls ein EU-Server nicht angeboten wird, sollten alternativ europäische Lösungen geprüft und ggf. umgesetzt werden. Bei bestehenden Auftragsverarbeitungsverhältnissen ist dringend sicherzustellen, dass bei einem Datentransfer in die USA oder andere Drittländer der betroffene Auftragsverarbeiter ein angemessenes Datenschutzniveau mithilfe von geeigneten Alternativen vorweisen kann. Eine erneute und kritische Prüfung der entsprechenden Verträge ist hierbei essenziell. Zudem ist der Auftraggeber (Datenexporteur) angehalten, die festgehaltenen Maßnahmen auch zu prüfen.

4. Verträge und Datenschutzhinweise aktualisieren

Es sollten alle relevanten Unterlagen geprüft und bei Bedarf angepasst werden. Dies gilt auch für das Verzeichnis der Verarbeitungstätigkeiten, soweit dort auf das Privacy Shield als Rechtsgrundlage abgestellt wurde.

5. Einwilligungen der Nutzer einholen

Bei Datenverarbeitungen, die auf einer Einwilligung beruhen, müssen die Nutzer transparent auf die Datenverarbeitung in den USA hingewiesen werden, bspw. mit einem Verweis in einem Cookie-Opt-In-Banner. Dabei ist jedoch zu beachten, dass eine Einwilligung in die Datenerhebung nicht automatisch die Übermittlung und Speicherung in die USA oder ein Drittland erlaubt. Auch hier gilt die Würdigung im Einzelfall.

Welche Rechtsfolgen können drohen?

Eine Datenübermittlung auf Basis des Privacy-Shield ist unzulässig. Wie auch bei unzureichenden Standardvertragsklauseln können die nationalen Aufsichtsbehörden eine Übermittlung untersagen und mit einem Bußgeld belegen. Dabei können die Bußgelder bis zu 20 Mio. Euro oder 4 % des Konzernjahresumsatzes betragen, je nachdem welcher der beiden Werte höher ist.

Es bleibt weiterhin spannend, wie sich die Lage entwickeln wird. An einem Nachfolgeabkommen zum Privacy-Shield wird zwar gearbeitet – jedoch ist noch unklar, wann dieses verabschiedet wird.

Insgesamt ist festzuhalten, dass derzeit das Risiko aus Verstößen im Zusammenhang mit der Datenübertragung in die USA lediglich reduziert, aber nicht verhindert wird. Es gilt aber aufgrund der Höhe der möglichen Sanktionen alles daran zu setzen, um das Risiko durch die aufgezeigten Maßnahmen zu reduzieren. Standardvertragsklauseln können helfen, müssen aber sachgerecht bewertet und angewandt worden sein.

Differential Privacy – zur Anonymisierung von Daten

Die größte Herausforderung bei der Durchführung von Big Data Projekten ist der Schutz personenbezogener Daten. Um den Verbraucherwünschen und gesetzlichen Vorgaben zu entsprechen, benötigen Unternehmen geeignete Anonymisierungstools. Da es jedoch verschiedene Anonymisierungsmechanismen für unterschiedliche Zwecke gibt, gilt es, die führenden Ansätze miteinander zu vergleichen.

Merkmalstypen

Zu anonymisierende Daten lassen sich in drei Merkmalsklassen einteilen: Identifikatoren, Quasi-Identifikatoren und sensitive Merkmale. Identifikatoren stellen Daten dar, die einer Person beinahe eindeutig bzw. eindeutig zugeordnet werden können (bspw. Nummer des Personalausweises). Hingegen stellen Quasi-Identifikatoren Merkmale dar, die in der Verknüpfung untereinander oder mithilfe des Einbezugs anderer legal erhältlicher Daten die Identifikation einer Person ermöglichen (bspw. PLZ, Geschlecht und Wohnort). Sensitive Merkmale sind ebenfalls schützenswerte Daten, die bei der Einsicht Dritter zu einem massiven Eingriff in die Privatsphäre oder anderen schwerwiegenden Konsequenzen führen können (z. B. Gesundheitsdaten).

Anonymisierung

Im Allgemeinen versteht man unter der Anonymisierung von Daten eine Veränderung der personenbezogenen Daten insofern, dass Einzelangaben über persönliche oder sachliche Verhältnisse - im Gegensatz zur Pseudonymisierung - nur sehr schwer einer oder sogar keiner natürlichen Person mehr zugeordnet werden können. Die Anonymisierung stellt - neben der Pseudonymisierung und Verschlüsselung - eine Möglichkeit zur Gewährleistung der Anforderungen an den Datenschutz dar. Dabei ist die Berücksichtigung der Aspekte Datensicherheit, Datenschutz sowie Datenqualität besonders relevant.

Mechanismen zur Anonymisierung – und Eignung wofür?

Es existieren unterschiedliche Verfahrensweisen zur Anonymisierung von Daten, wobei eine Grundvoraussetzung das Abhandensein von Identifikatoren darstellt.

Wenn es um Webanalysen geht, kann z. B. das **endgültige Löschen des letzten Oktetts einer IP-Adresse** (bei Google Analytics erfolgt dies durch das Verwenden von anonymizeIP) eine wirkungsvolle Anonymisierung darstellen. Dabei ist zu beachten, dass in den übrigen zu der jeweiligen IP-Adresse gespeicherten Daten keine eindeutigen Merkmale enthalten sind, die eine eindeutige Identifikation zulassen.

Auch kann man sich des **Data Masking** (Datenmaskierung) bedienen, welche weiter geht als die reine Anonymisierung und Pseudonymisierung von Personen- und Adressdaten. Im Rahmen dessen wird eine strukturell ähnliche, aber inauthentische Version der Daten erstellt. Ziel der Datenmaskierung ist die Data Leakage Prevention oder Data Loss Prevention – also die Verhinderung von Datenlecks und Datenverlusten.

Eine Anonymisierung von **Datenbanken** kann z. B. mithilfe von Programmen wie Anonimatron (Open-Source-Lösung auf Java-Basis) vorgenommen werden, bei denen u. a. E-Mail-Adressen durch frei erfundene ersetzt werden (dies geht eher in die Richtung der Pseudonymisierung). Sollen Dateinamen, Verzeichnisnamen und Datenelemente anonymisiert werden, bietet sich z. B. DICOM Anonymizer&Masker an. Die nachträgliche Anonymisierung ist demnach möglich.

Bei **Marktforschungen** ist die Erhebung von Daten das angestrebte Ziel der Untersuchung. Damit jedoch Teilnehmer der Studien anonym bleiben können, kann der Befragte angeben, dass er möchte, dass die IP-Adresse entfernt wird, bevor die Antworten gespeichert werden. Dadurch kann auch der Umfrageteilnehmer vor Aufdeckung der Identität geschützt werden. Auch gibt es die Möglichkeit, alle personenbezogenen Daten vor der endgültigen Speicherung so zu überarbeiten, dass diese als anonymisiert gelten können.

Insb. für Unternehmen sollte der „anonyme Kunde" ein angestrebtes Ziel darstellen. Eine Vorgehensweise etwa der Aircloak GmbH zeigt, dass sich **Nutzerdaten anonymisieren** lassen und so durch sog. Privacy Enhancing Technologies (PET) bisherige Prozesse zur Anonymisierung von Daten durch entsprechende automatisierte Lösungen ersetzt werden können.

Differential Privacy

Das Anonymisierungstool Differential Privacy kann in Unternehmen verwendet werden, in denen besonders viele Daten verarbeitet werden. Es sieht eine Datenanonymisierung durch das Einpflegen von randomisiertem Rauschen vor. Je mehr Rauschen hinzugefügt wird, desto undurchsichtiger und verzerrter wird der Datensatz. Man kann dadurch immer weniger Details erkennen - bis hin zur vollständigen Unkenntlichkeit der (als privat geltenden) Datensätze.

Differential Privacy stellt, im Gegensatz zu ethischem oder rechtlichem Schutz persönlicher Daten, eine mathematische Definition von Privatsphäre dar. Ein Parameter (Epsilon) steuert, wie viele Informationen über einen Benutzer offengelegt werden; indem man diesen Wert einstellt, bestimmt man die Menge des Rauschens, die den Daten hinzugefügt werden muss. Je stärker das Rauschen eingestellt ist, desto höher ist die Sicherheit.

Der Schutz der Privatsphäre wird demnach durch die erzeugte Unsicherheit gewährleistet, weil alle anonymisierten Daten – wegen der Randomisierung – mit gleicher Wahrscheinlichkeit wahr sowie falsch sein könnten. Auch wenn einem Angreifer alles über die Daten bekannt ist, kann er die Daten nur mit Mühe einer und im Regelfall keiner Identität zuordnen. Es kann nicht einmal ermittelt werden, ob eine gewisse Person in gespeicherten Daten vorkommt.

Problematisch wird es, wenn dem Angreifer der Schlüssel des randomisierten Rauschens bekannt ist. Dadurch könnte er Daten z. B. über die Anzahl einer befragten Gruppe etc. herausfiltern. Das ist ein Merkmal der differentiellen Privatsphäre – die Informationen jeder Einzelperson können geschützt werden. Sobald jedoch Details bekannt sind, wie z. B. die Frequenz des Rauschens, die zu den Daten hinzugefügt wurde, sind häufig statistische Schätzungen wie Zählungen, Mittelwerte oder sogar fortgeschrittenes maschinelles Lernen möglich.

Grundsätzlich wird ein niedriger Wert von Epsilon (zwischen 0.1 und 1) empfohlen, wodurch jedoch nur wenige Anfragen (ca. 12) an das Datenmaterial möglich werden. Die bei Google und Apple verwendeten Mechanismen lösen das Problem der verminderten Anfragemöglichkeiten, in dem z. B. Annahmen über die fehlende Verbundenheit von Attributen getroffen und wiederum welche für dasselbe Attribut über Zeit getroffen werden. Somit ist eine unbegrenzte Anzahl an Anfragen ermöglicht – großes Rauschen und Korrelationen zwischen Attributen können dadurch nicht mehr ausgemacht werden.

Für die meisten analytischen Auswertungen ist jedoch ein niedrigeres Rauschen, also mehr Detailgenauigkeit, notwendig. Deshalb besitzen viele Implementierungen von Differential Privacy einen Epsilonwert von 10, wodurch die Privatsphäre der Nutzer jedoch nicht mehr gewährleistet werden kann. Andererseits reduziert ein geringer Epsilonwert den Informationsgehalt von Datensätzen.

Weshalb anonymisieren?

Zwar rufen Datenschützer stets zur Anonymisierung, Datenvermeidung und Datensparsamkeit auf, um die Verarbeitung personenbezogener Daten auf ein Minimum zu reduzieren, dennoch sind Unternehmen nicht verpflichtet, die Löschung jeglichen Personenbezugs der betriebsinternen Datenbestände vorzunehmen. Zum Teil stehen dem darüber hinaus insb. gesetzliche Aufbewahrungsfristen entgegen.

Trotzdem sollte jedem Unternehmen der Schutz der Kundendaten wichtig sein. Der unberechtigte externe Zugriff auf den Kundenstamm kann auch zur Schädigung des eigenen Unternehmens führen.

Die im eigenen Unternehmen durchgeführte Anonymisierung von Daten in Bezug auf die Einhaltung rechtlicher Vorschriften sowie das Entgegenkommen auf die Verbraucherwünsche stellt einen Vorteil dar. Interessant wird es für jeden Unternehmer besonders hinsichtlich der Einhaltung der DSGVO, da für alle vollständig anonymisierten Daten z. B. die Zweckbindung von Daten oder die Einhaltung von Löschpflichten, entfallen. Dies stellt eine enorme Reduzierung des bürokratischen Aufwandes dar.

Hinweis: Differential Privacy lässt sich mithilfe von kostenloser Anonymisierungssoftware testen. Eine davon ist z. B. PSI, eine Implementierung des Harvard Privacy Tools Projects.

Gesundheitswesen: Das neue Patientendaten-Schutz-Gesetz – Auswirkungen für Krankenhäuser im Informationssicherheitsumfeld

„Schluss mit der Zettelwirtschaft": Der Bundesrat hat am 18.9.2020 das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG) gebilligt, das der Bundestag bereits Anfang Juli verabschiedet hatte. Am 19.10.2020 wurde es im Bundesgesetzblatt veröffentlicht. Ziel des PDSG ist eine stärkere Digitalisierung im Gesundheitsbereich unter stetiger Anpassung im Hinblick auf den technologischen Fortschritt. Darunter sind konkretisierende Vorgaben im Zusammenhang mit der elektronischen Patientenakte (ePa), dem E-Rezept, Vorgaben zur Sicherheit in der Telematikinfrastruktur, aber auch höhere Anforderungen zur IT-Sicherheit bzw. Informationssicherheit in Krankenhäusern.

Änderungen durch das PDSG

Beim PDSG handelt es sich um ein Artikel-Gesetz, d. h. das PDSG ändert inhaltlich eine Vielzahl anderer Gesetze, so z. B. die Sozialgesetzbücher (speziell SGB V), das Apothekengesetz oder das Krankenhausfinanzierungsgesetz.

Nachfolgend haben wir die wichtigsten Punkte in Auszügen dargestellt:

- **ePa:** Die elektronische Patientenakte ist nicht neu. Nach bereits geltendem Recht müssen Krankenkassen eine elektronische Patientenakte (ePa) ab 2021 anbieten. Ab 2022 erhalten auch die Versicherten selbst Zugriff auf ihre ePa. In der ePa können entsprechende Dokumente und Daten gesammelt und abgelegt werden (z. B. Befunde, Röntgenbilder, Vorsorgeuntersuchungen, etc.). Bei einem Kassenwechsel können Versicherte ihre Daten aus der ePA übertragen lassen. Die Nutzung der ePa ist für den Versicherten freiwillig. Die derzeitige Ausgestaltung der ePa steht in datenschutzrechtlicher Hinsicht in der Kritik, die auch vom Bundesdatenschutzbeauftragten (BfDI) geteilt wird. So können zum Start der ePa 2021, z. B. nur rudimentäre Zugriffsrechte durch den Versicherten vergeben werden. Im Konkreten bedeutet dies, dass zwar die Versicherten festlegen können, welche Daten überhaupt in der Patientenakte gespeichert werden dürfen und welcher Arzt die Daten/Dokumente einsehen darf, detailliertere Einstellungsmöglichkeiten der Zugriffe, differenziert nach Arzt und Dokument, sind jedoch erst ab 2022 vorgesehen.

- **E-Rezept:** Mit Einführung des E-Rezepts können Ärzte Rezepte direkt digital erstellen und verschlüsselt speichern. Der Patient kann das Rezept dann über eine App mittels eines Schlüssels (z. B. per QR-Code) bei jeder Apotheke einlösen. Die Einführung des E-Rezepts ist bereits mit dem „Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV)", das am 16.8.2019 in Kraft getreten ist, erfolgt. Das PDSG ergänzt das GSAV nicht nur im Hinblick auf die sichere Telematikinfrastruktur, sondern legt auch die verbindliche Einführung des E-Rezeptes für Anfang 2022 fest. Die genauen technischen und prozessualen Vorgaben sind aber derzeit noch nicht vollumfänglich spezifiziert.

- **Vorgaben zur Sicherheit in der Telematikinfrastruktur:** Unter Telematik wird die Vernetzung verschiedener IT-Systeme sowie die Verknüpfung von Informationen aus unterschiedlichen Quellen bezeichnet. Nach Vorstellung des Gesetzgebers vernetzt die Telematikinfrastruktur (TI) alle Akteure des Gesundheitswesens (z. B. Ärzte, Krankenhäuser und Krankenkassen) und stellt einen sektoren- und systemübergreifenden sowie sicheren Austausch von Informationen und medizinischen Daten sicher (z. B. Einsicht in die ePa, Austausch des E-Rezepts, etc.). Es handelt sich dabei um ein geschlossenes Netz, zu dem nur registrierte Nutzer Zugang erhalten. Im Hinblick auf neue Komponenten und Dienste, die in der TI genutzt werden, müssen gemäß den Anforderungen des PDSG diese Komponenten und Dienste eine Zulassung durchlaufen. Die Zulassung setzt als Nachweis eine Sicherheitszertifizierung der Komponente und/oder des Dienstes voraus. Anbieter müssen für ihre Komponenten und Dienste zudem unter Berücksichtigung des Stands der Technik, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit umsetzen. Vorgaben, die mit den organisatorischen und technischen Vorkehrungen in Verbindung stehen, müssen je nach Relevanz von den Teilnehmern der TI berücksichtigt werden. So müssen z. B. auch Arztpraxen sicherstellen, dass nur noch zugelassene, d. h. zertifizierte Komponenten zur Anbindung an die TI genutzt werden.

Die vorangegangenen Punkte verdeutlichen: Das PDSG verlangt einen stärkeren Fokus auf die Informations- und IT-Sicherheit. Dies hat erwartungsgemäß erhebliche Auswirkungen auf die Dienstleister und Lieferanten von Komponenten bzw. Anwendungen für die TI. Was häufig jedoch unterschätzt wird, sind die technischen und organisatorischen Anforderungen, die an die operativen und nicht aus der IT stammenden Teilnehmer der TI, wie z. B. die Ärzte und Krankenhäuser, gestellt werden.

Informationssicherheit bzw. IT-Sicherheit nun für alle und nicht nur für KRITIS-relevante Krankenhäuser

Durch das PDSG ergab sich eine weitere weitreichende Änderung in § 75c Sozialgesetzbuch – Fünftes Buch (SGB V). Diese betrifft alle Krankenhäuser und legt den Fokus auf die Informationssicherheit. Nachdem der Gesetzestext sehr plakativ darstellt, dass Informationssicherheit nun für alle Krankenhäuser gilt, sofern diese nicht KRITIS Betreiber sind und sich demnach noch zusätzlich prüfen lassen müssen, haben wir die drei Absätze des § 75c SGB V hier abgedruckt:

(1) Ab dem 1.1.2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

(2) Die Krankenhäuser können die Verpflichtungen nach Abs. 1 insb. erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Abs. 2 des BSI-Gesetzes festgestellt wurde.

(3) Die Verpflichtung nach Abs. 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

Bisher ergaben sich umfassende Anforderungen in Bezug auf die IT-Sicherheit bzw. Informationssicherheit für Krankenhäuser zum einen im Wesentlichen aus § 8a BSIG für sog. „Kritische Infrastrukturen" (Krankenhäuser mit mindestens 30.000 vollstationären Behandlungsfällen im Jahr), zum anderen aus § 75b SBG V für vertragsärztliche Leistungen, die im Krankenhaus erbracht werden. In diesem Zusammenhang mussten Systeme und Prozesse der betreffenden Krankenhäuser die Vorgaben der Kassenärztlichen Bundesvereinigung (KBV) oder die Anforderungen des Branchenspezifischen Sicherheitsstandards (B3S) der Deutschen Krankenhausgesellschaft sicherstellen.

Mit Ausnahme der Melde- und Prüfungspflicht sind die neuen Vorgaben des § 75c SGB V somit nun für alle Krankenhäuser verbindlich umzusetzen. Die Vorgaben zur IT-Sicherheit (vgl. § 75c SGB V […] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit […] [ihrer] Systeme, Komponenten oder Prozesse zu treffen […]) sind somit nicht mehr auf die Krankenhäuser im KRITIS Umfeld beschränkt. Jedes Krankenhaus ist somit angehalten, ausreichend Maßnahmen nach dem Stand der Technik für die Aufrechterhaltung von Versorgungsdienstleistungen zu treffen und diese Maßnahmen entsprechend zu steuern.

Als Orientierung zur Umsetzung dieser Anforderungen kann auch für Krankenhäuser im Nicht-KRITIS Umfeld der branchenspezifische Sicherheitsstandard (B3S) für die Gesundheitsversorgung in Krankenhäusern herangezogen werden. Der B3S umfasst dabei 168 Anforderungen, die umzusetzen sind, um die Sicherstellung und die Aufrechterhaltung der benötigten Versorgungsprozesse zu gewährleisten. Dabei ist festzuhalten, dass in diesem Zusammenhang nicht nur auf die TI, sondern auch auf weitere für die Versorgungsdienstleistung notwendigen Prozesse, Anwendungen und Infrastrukturkomponenten abzustellen ist.

Zusammengefasst sind Krankenhäuser verpflichtet, organisatorische und technische Maßnahmen zur Sicherstellung der IT- und Informationssicherheit umzusetzen. Entsprechend der Vorgaben des B3S und auch aus Erfahrung anderer Bereiche und Branchen, die ähnliche Forderungen umzusetzen hatten, kann eine Umsetzung der Anforderungen des § 75c SGB V nur mit dem Aufbau eines umfassenden Informationssicherheitsmanagements (ISMS) gelingen. Im Hinblick auf die sehr kurze Umsetzungsfrist bis 31.12.2021 sollten Krankenhäuser zeitnah mit der Umsetzung der Anforderungen beginnen.

Fazit

Mit dem PDSG gehen Änderungen in unterschiedlichen Branchen im Gesundheitssektor einher. Speziell Anforderungen an die IT-Sicherheit bzw. Informationssicherheit finden stärkere Beachtung und sollten zeitnah umgesetzt werden. Dies betrifft im Hinblick auf die TI sowohl die Arztpraxis von „nebenan" als auch Krankenkassen.

Speziell Krankenhäuser sollten vor dem Hintergrund der Anforderungen des § 75c SGB V zumindest den Stand der Umsetzung der Informationssicherheit im eigenen Haus prüfen und ggf. ein ISMS implementieren oder anpassen. Es gilt, die verbleibende Zeit in allen Bereichen effizient zu nutzen.

Bei der Implementierung eines Informationssicherheitsmanagementsystems sollte keine isolierte Stand Alone-Umsetzung vorgenommen, sondern zur Steigerung der Effizienz ein integrierter Managementansatz gewählt werden. Bei der Umsetzung ganzheitlicher und integrierter Managementsysteme, wie z. B. ISMS/DSMS/KRITIS, haben wir aus unserer Erfahrung eine effiziente Herangehensmethodik erarbeitet.

Ergänzend weisen wir darauf hin, dass das Bundeskabinett ein Förderprogramm für die Krankenhaus-IT beschlossen hat. Hierbei sollen Krankenhausträger beim Abbau von Defiziten bei der Digitalisierung und Vernetzung unterstützt werden. Zu den weiteren Förderbereichen zählen auch Investitionen in die Informationssicherheit und das Notfallmanagement, die zur Stärkung der Versorgungsstruktur beitragen.

EN 303 645 – Einhaltung von IoT-Sicherheitsstandards

Die Welt der „Smart Devices“ und „Internet of Things“ (IoT) befindet sich weiterhin auf der Überholspur und doch waren die Anforderungen dafür verschwindend gering, da es faktisch eine lange Zeit keine strikten Regulierungen gab. Mit Entwicklung neuer Technologien entstehen jedoch auch Sicherheitstechnologien und gleichzeitig Normen, Regularien, Standards und Vorschriften, welche diese neuen Technologien in geordnete Bahnen lenken und diesen entsprechende Vorgaben zur Einhaltung geben sollen.

ISO / IEC 30141:2018-08

Im Jahr 2018 wurde die Richtlinie ISO / IEC 30141:2018-08 „Internet of Things (IoT) - Reference Architecture“ erlassen. Ziel der Richtlinie ist, die Sicherheit und Interoperabilität von IoT-Systemen und die Vertraulichkeit der verarbeiteten Daten zu gewährleisten. Dazu enthält die Norm bspw. ein standardisiertes Vokabular, wiederverwendbare Concept Maps und Best Practices für die Branche.

ETSI TS 103 645

Das European Telecommunications Standards Institute (ETSI), bei dem es sich um eine unabhängige Non-Profit-Organisation handelt, die bei der Entwicklung von technischen Standards in der IT- und Telekommunikationsbranche unterstützt, hat in 2019 die technische Spezifikation 103 645 („Cyber Security for Consumer Internet of Things“) für IoT-Geräte und -Dienste veröffentlicht.

Mittels der ETSI TS 103 645 werden zumindest grundlegende Anforderungen an die IT-Security gestellt, die erfüllt werden müssen. Insgesamt sind folgende Cyber-Sicherheitsbestimmungen für Verbraucher-IoT-Geräte definiert worden:

1. Keine Standardpasswörter verwenden (No universal default passwords)
2. Richtlinie zur Offenlegung von Schwachstellen implementieren (Implement a means to manage reports of vulnerabilities)
3. Software auf dem aktuellen Stand halten (Keep software updated)
4. Zugangsdaten und sicherheitsrelevante Daten sicher speichern (Securely store credentials and security-sensitive data)
5. Sicher kommunizieren (Communicate securely)
6. Angriffsflächen minimieren (Minimize exposed attack surfaces)
7. Software-Integrität gewährleisten (Ensure software integrity)
8. Schutz von personenbezogenen Daten gewährleisten (Ensure that personal data is protected)
9. Systeme ausfallsicherer gestalten (Make systems resilient to outages)
10. System-Telemetriedaten überwachen (Examine system telemetry data)
11. Verbrauchern die einfache Löschung personenbezogener Daten ermöglichen (Make it easy for consumers to delete personal data)
12. Installation und Wartung von Geräten vereinfachen (Make installation and maintenance of devices easy)
13. Eingabedaten überprüfen (Validate input data)

EN 303 645

Der Europäische Standard (EN) 303 645 baut auf den vorherigen technischen Standard ETSI TS 103 645 auf und dient als neuer weltweit anwendbarer Mindestsicherheitsstandard für die sichere Entwicklung (Security by Design) von IoT-Geräten. Der Standard wurde am 30.6.2020 unter Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch die ETSI veröffentlicht. Er spezifiziert dabei die zuvor aufgeführten 13 grundlegenden Bestimmungen für die Sicherheit von IoT-Geräten.

IT-Sicherheitskatalog für Energieerzeuger gemäß § 11 Abs. 1 b EnWG

Der IT-Sicherheitskatalog gemäß § 11 Abs.1a Energiewirtschaftsgesetz (EnWG) wurde bereits im Jahr 2015 veröffentlicht. Das Ziel dabei ist die Etablierung eines angemessenen Schutzes gegen Bedrohungen für sicherheitsrelevante Informations- und Kommunikationstechnologien im Energiesektor. Dadurch soll eine sichere Energieversorgung gewährleistet werden. Im IT-Sicherheitskatalog werden konkrete Anforderungen und Maßnahmen für einen sicheren Anlagenbetrieb aufgeführt.

Da jedoch auch Betreiber von bestimmten Energieanlagen, wie bspw. größere Erzeugungsanlagen erfasst werden sollen, wurde im Jahr 2018 die Vorschrift um den Abs. 1b erweitert. Bis zum 31.3.2021 müssen alle betroffenen Betreiber ein Zertifikat bei der Bundesnetzagentur vorlegen. Die Zertifizierung darf nur von Zertifizierungsstellen durchgeführt werden, die durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditiert sind.

Tatsächliche Neuerung oder doch nur Erweiterung?

Zwei Aspekte sind bei der Einführung des Abs. 1b genauer zu betrachten: der Adressatenkreis, der den Sicherheitskatalog anwenden muss und die Definition des Geltungsbereichs.

Gemäß § 11 Abs. 1a EnWG gelten die Vorgaben für Netzbetreiber sowie für kritische Infrastrukturen, jedoch finden die Schwellenwerte der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) keine Anwendung. Dies ändert Abs. 1b, da die Schwellenwerte der BSI-KritisV nun zu beachten sind. Betreiber, die die genannten Schwellenwerte erreichen bzw. überschreiten, müssen die Anforderungen des § 11 Abs. 1b EnWG erfüllen, da die Energieversorgung nicht nur von den Strom- und Gasnetzbetreibern gewährleistet wird. Entscheidend ist auch die Summe der Energieanlagen.

Die genannten Betreiber sind zum Aufbau und zum Betrieb sowie zum Audit und zur Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) nach DIN ISO/IEC 27001 verpflichtet. Dadurch sollen IT-sicherheitstechnische Mindeststandards gewährleistet werden. Dies empfiehlt sich jedoch auch bereits für Betreiber, die die Schwellenwerte nicht erreichen, da im Rahmen der Evaluierung der BSI-KritisV mit einer Senkung der Schwellenwerte gerechnet wird.

Bislang war eine Betrachtung der Netzsegmentierung ausreichend. Hinsichtlich des Geltungsbereiches fordert § 11 Abs. 1b EnWG nun die Zuordnung der Anwendungen, Systeme und Komponenten zu sechs verschiedenen Zonen. Dies gilt für Systeme, die für die Prozessführung und im Leitstand eingesetzt werden, ebenso wie für Büro- und Verwaltungssysteme. Die Einteilung in die verschiedenen Zonen erfolgt nach der jeweiligen Bedeutung für den sicheren Anlagenbetrieb.

Konformitätsbewertungsprogramm

Knapp zwei Jahre nach der Einführung des § 11 Abs. 1b EnWG veröffentlichte die DakkS nun im August 2020 das Konformitätsbewertungsprogramm. Darin werden die spezifischen Anforderungen an die Zertifizierungsstellen sowie der Umfang des Audits festgelegt. Auditoren sind unter anderem dazu verpflichtet, eine durch die Bundesnetzagentur anerkannte Schulung zu den Grundlagen der Erzeugung und leitungsgebundenen Versorgung mit Strom und Gas zu absolvieren. Das Programm richtet sich grundsätzlich an die Zertifizierungsstellen, es ist jedoch auch für die Betreiber interessant. Denn es wird deutlich, dass die Grundlage für die Zertifizierung etablierte Standards, wie DIN ISO/IEC 27001 für ISMS sowie ISO/IEC 27019 für den Maßnahmenkatalog im Bereich Energienetze, sind.

FAQ zur Umstellung auf SAP S/4HANA- Teil 1

SAP S/4HANA ist nicht nur ein Nachfolger einer beliebten Business Suite, sondern ein vollständiges neues System mit einer neuen und modernen Architektur. Und, wie es Veränderungen so an sich haben, werfen sie viele Fragen auf.

Im Zuge unserer Webinar-Reihe Fokus IT zur „Einführung SAP S/4HANA" sowie unserer durchgeführten Projekte werden wir mit einer Reihe von Fragen konfrontiert, die im Zweifel nicht in jedem Ratgeber zur Migration erläutert werden.

Ziel dieser neu eingeführten Reihe, die wir in den kommenden Ausgaben des novus IT fortsetzen möchten, um Ihnen den Umstieg auf SAP S/4HANA zu erleichtern, ist daher diese Reihe mit Frequently Asked Questions (FAQs).

(1) Wie gehe ich mit den potenziell hohen Kosten für die In-Memory-Lösung für SAP S/4HANA um?

Viele Unternehmen schrecken vor einer Einführung von SAP S/4HANA zurück, da sie sich vor zu hohen Kosten fürchten. Die Kosten entstehen hauptsächlich durch das Volumen, da SAP S/4HANA pro Gigabyte Datenbank lizensiert wird. Bei den Datenmengen, die in Unternehmen vorhanden sind, können die Kosten tatsächlich schnell explodieren. Auch das jährliche Datenwachstum muss bedacht werden, so wird bspw. von einer Erhöhung von ca. 5 bis 15 % pro Jahr ausgegangen. Wie viel SAP jedoch pro Gigabyte erheben wird, ist noch nicht bekannt und die Meinungen gehen in diesem Zusammenhang noch stark auseinander.

Es gibt durchaus Möglichkeiten, um die Kosten einzugrenzen. Von existenzieller Bedeutung ist die Data Footprint Reduction, wobei es sich um eine Ansammlung von Techniken, Technologien, Anwendungen und Best Practices-Ansätzen handelt, die zur Bewältigung der Herausforderungen beim Management des Datenwachstums eingesetzt werden. Das gesamte Data Lifecycle Management für unmittelbar verfügbar vorgehaltene Daten muss überarbeitet werden. Dazu gehört u. a. das Data Temperature Management (siehe Frage 2). Zudem sollten temporäre und redundante Dateien automatisch erkannt und gelöscht werden. Das aktuelle Konzept der Datenverfügbarkeit und der Datenarchivierung muss überarbeitet werden; dies kann gegebenenfalls auch über eine Drittsoftware erfolgen. Eventuell kann auch eine Auslagerung der Langzeitdatenspeicherung sinnvoll sein. Es stehen unzählige Anbieter zur Verfügung, darunter bspw. AWS, MS Azure und Google Cloud. Die Abrechnung erfolgt meist als Pauschale, zusätzlich wird eine Gebühr für die Datenbank-Nutzung fällig.

Neben den Softwarekosten kommen die Kosten für die Anschaffung neuer, von der SAP zertifizierte Hardware hinzu. Durch die In-Memory-Technologie wird bei SAP S/4HANA vergleichsweise viel Arbeitsspeicher benötigt. Es ist daher ratsam, bereits bei der Einführung bzw. im Zuge des Umstiegs eine Cluster-Strategie für die Infrastruktur zu planen und zu kalkulieren. Infrage kommt entweder ein Cluster Scale Up oder ein Cluster Scale Out. Das Cluster Scale Up zeichnet sich dadurch aus, dass die verwendeten Server durch Hardwareupgrades erweitert werden. Durch den Einbau von mehr Arbeitsspeicher können die Server dann mit bis zu 1,5 Terabyte pro Sockel „mitwachsen". Beim Cluster Scale Out hingegen erfolgt die Erweiterung durch die Einbindung neuer Maschinen, da SAP S/4HANA auf mehreren physischen Maschinen laufen kann.

(2) Muss ich alles „In-Memory" vorhalten oder darf ich auch diverse (alte) Daten archivieren und per Abruf bereitstellen?

SAP verfügt über ein sog. Data Temperature Management. Je nach Zugriffshäufigkeit werden Daten in die Kategorien „hot", „warm" oder „cold" eingestellt. Daten in der Kategorie „cold", auf die also eine bestimmte Zeit nicht zugegriffen wurde, werden archiviert (in den Langzeitspeicher übergegeben). Diese historischen Daten müssen also grundsätzlich nicht „In-Memory" vorgehalten werden. Eine Archivierung der historischen Daten ist möglich und führt damit durch die Reduzierung des Speicherplatzes zu einer Kostensenkung bzw. vermeidet eine Kostenerhöhung.

Bereits im Zuge der Migration sollte die Archivlösung (Langzeitspeicherung von Daten/ Historisierung von Daten) geplant und implementiert werden. Die Datenmenge kann bereits durch die Löschung nicht mehr verwendeter Reports oder auch durch die Archivierung nicht mehr benötigter Daten erheblich reduziert werden. Zusätzlich können Sanity Checks (Plausibilitätsprüfungen) der Daten hilfreich sein: Dabei ist zu klären, für welche Daten eine Lagerung außerhalb von HANA effektiver und einfacher sein könnte.

Bei der Einteilung der Daten handelt es sich jedoch nicht nur um eine Kostenfrage, sondern auch um eine Frage der Leistungsstärke. Denn je mehr Daten des Altsystems archiviert werden, desto leistungsstärker ist das neue System SAP S/4HANA bei seiner Einführung. Die Übertragung der historischen Daten erfolgt über eine externe Schnittstelle. Da für die historischen Daten nicht zwingend ein schnellstmöglicher Zugriff notwendig ist, können diese in der Archivlösung gehalten werden.

(3) Wie wird SAP HCM in SAP S/4HANA übernommen bzw. abgebildet?

Zum jetzigen Stand (Oktober 2020) gibt es noch kein SAP S/4HANA HCM, allerdings wurde dies für das dritte Quartal 2022 angekündigt. Als kleiner Teaser vorab: Der Funktionsumfang soll nach aktuellem Stand identisch zu dem bereits aus der R/3-Welt bekannten SAP HCM sein und auch ein SAP Travel Management ist geplant. In der Zukunft wird der Hauptfokus von SAP weiterhin auf dem neuen HCM SAP SuccessFactors liegen, wobei durch das Einlenken SAP Kunden nun zwei Möglichkeiten offenstehen und nicht mehr zwangsweise in die Public Cloud zu SuccessFactors gewechselt werden muss.

Für den Übergang hat SAP das SAP S/4HANA HCM Compatibility Pack entwickelt. SAP User können diese Lösung bis Ende 2025 nutzen. Über die Kosten, die diese Übergangslösung mit sich bringt, machte SAP bislang noch keine Angaben.

(4) Wie vollständig ist der Funktionsumfang bei S/4 Single Tenant im Vergleich zu Multi Tenant?

Die beiden Betriebsmodelle Single Tenant und Multi Tenant unterscheiden sich vor allem im Hinblick auf die Anpassbarkeit der Prozesse und im Customizing des SAP S/4. In der Single Tenant Version kann der Benutzer seine eigene Systemlandschaft auf Basis der entsprechenden Cloud-Infrastruktur kreieren. Betriebswirtschaftliche Prozesse, wie Finanzen, Personal, Beschaffung und Vertrieb, sind konfigurierbar und anpassbar. Die Architektur wird ausschließlich von einem Kunden genutzt; es muss eine eigene Softwareinstanz und Infrastruktur angemietet werden. Bei der Migration ist nur der Greenfield-Ansatz möglich. Das Single Tenant Betriebsmodell kann von allen Geschäftsbereichen und in sämtlichen Branchen genutzt werden. Diese Version ist deutlich flexibler, jedoch spiegelt sich das auch in den höheren Kosten (u. a. für Lizenzen) wider.

Für Multi Tenant User wird eine Public Cloud Infrastruktur genutzt. Die bereits oben genannten Prozesse sind nur noch eingeschränkt konfigurierbar, es werden zudem Best Practices für ausgewählte Prozesse durch SAP zur Verfügung gestellt. Es teilen sich mehrere Kunden eine Softwareinstanz und Infrastruktur. Durch eine Teilung je Kunde ist sichergestellt, dass nicht auf Daten anderer Kunden zugegriffen werden kann. Die Nutzung bleibt bislang nur den Dienstleistungs- und Komponentenfertigungsbranchen vorbehalten, die Einrichtung der Nutzung für weitere Branchen ist allerdings in der Planung. Ebenso wie bei der Single Tenant Version kommt für die Migration nur der Greenfield-Ansatz infrage.

(5) Wird es in S/4 weiterhin die Transaktion SA38 (Aufruf von Reports) und SE16 (Tabelleninhalte anzeigen) geben?

Eine gute Nachricht für alle, die sich die Transaktionscodes gut eingeprägt haben: Ja, die Transaktionscodes SA38 und SE38 bleiben zunächst unverändert erhalten. Die Transaktion SE16 wurde bereits vor S/4HANA von SE16N für den Übergang bzw. SE16H als neueste Version abgelöst, funktioniert jedoch weiterhin. SE16H bietet sogar noch weitere Funktionen: Datenbankverbindung, Aggregation und Outer Join.

Zudem gibt es die Möglichkeit, die Transaktionscodes aus SAP R/3 zu SAP S/4 übersetzen zu lassen. Dafür wird der Transaktionscode SE16 (N/H) genutzt.

(6) Welche wesentlichen Lizenzmodelle gibt es?

SAP stellt die Kunden bei der Lizensierung vor die Wahl zwischen Contract Conversion und Product Conversion. Die Frage, welches Modell empfehlenswert ist, ist unternehmensindividuell zu beantworten. Die Contract Conversion ermöglicht es, Altlasten im Rahmen der Umstellung auf S/4 loszuwerden, indem nicht genutzte SAP Produkte eliminiert werden. Insb. für Unternehmen, die Umstrukturierungen hinter sich haben, können so Überlizensierungen vermieden und somit Kosten eingespart werden. Der SAP-Lizenzvertrag kann entsprechend an den aktuellen und zukünftigen Bedarf angepasst werden. Im Anschluss erfolgt eine Verrechnung der Kosten der definierten Lizenzen mit dem bisherigen Lizenzwert. Bezahlt werden muss am Ende nur die Differenz. Da eine „Rückgabe“ oder ein „Umtausch“ der SAP-Lizenzen ansonsten nicht möglich ist, sollte diese Chance im Bedarfsfall genutzt werden.

Die zweite Option ist die Product Conversion; hier bleibt der vereinbarte Vertrag grundsätzlich bestehen. Durch den Kauf zweier Lizenzkomponenten erfolgt ein Update auf SAP S/4HANA. In diesem Modell wird ein einmaliger Pauschalbetrag von 9.000 Euro fällig. Die bestehende SAP ERP Lizenz wird in eine SAP S/4HANA Lizenz umgewandelt. Diese Umwandlung ist allerdings mit Vorsicht zu genießen, denn sie beinhaltet nur die Lizenzen, die zum S/4HANA Core System gehören. Für die Engines, wie bspw. Cash Management, muss die Lizenz separat erworben werden, eventuell ist eine Anrechnung jedoch möglich.

Technische Herausforderungen bei der Einführung von bzw. der Migration auf SAP S/4HANA

Die ursprüngliche „Deadline" zur Einführung von SAP S/4HANA wurden seitens SAP von 2025 auf 2027 verlängert. Das Jahr 2027 erscheint heute noch in weiter Ferne. Mit der Planung für den Umstieg sollte jedoch schon jetzt begonnen werden, denn spätestens 2022 wird von einem Ressourcenengpass auf der Beraterseite ausgegangen.

Im Rahmen unseres ersten novus IT in diesem Jahr haben wir Ihnen bereits die Roadmap sowie mögliche Transformationszenarien auf SAP S/4HANA (Stichwort: Greenfield, Brownfield und Bluefield) vorgestellt. In unseren Webinaren haben wir Ihnen aufgezeigt, welche die größten Herausforderungen bei der Einführung von SAP S/4HANA sind. Bei der Einführung gilt es, neue technische (z. B. Cloud-Infrastrukturen) und prozessbezogene Herausforderungen (z. B. das Verbleiben im SAP S/4 Standard) zu beachten. Nachfolgend möchten wir insb. die technischen Voraussetzungen und Herausforderungen darstellen.

Hintergrund

Mit der Veröffentlichung von der SAP Business Suite powered by SAP HANA im Jahr 2013 hat SAP die volle Funktionalität der SAP Business Suite (SAP ERP, SAP CRM, SAP SCM, SAP BW, etc.) auf die neue SAP HANA Plattform gebracht. Im Jahr 2014 begann SAP mit der Entwicklung einer neuen Business Suite. Als Beginn ist S/4HANA Finance (ehemals SAP Simple Finance) anzusehen. Bei S/4HANA Finance wurde der gesamte Code der klassischen SAP ERP Anwendungen SAP FI und SAP CO komplett neu geschrieben, damit diese nativ auf SAP HANA laufen. Nativ bedeutet dabei, dass der neu geschriebene Code nur auf der SAP HANA Datenbank lauffähig ist.

SAP S/4HANA ist kein einzelnes monolithisches Produkt, sondern kann zu einer kompletten Business Suite zusammengestellt werden. Im Mittelpunkt steht das SAP S/4HANA Enterprise Management, welches aus der Perspektive des Funktionsumfangs mit dem SAP ERP aus der klassischen SAP Business Suite verglichen werden kann. Es lässt sich somit mit den grundlegenden Komponenten beginnen, und sukzessive – wenn erforderlich – erweitern.

2027: END OF LIFE BUSINESS SUITE 7 (INKL. ERP 6.0)

SAP R/3	SAP ECC (ERP)	HANA	S/4HANA
Zum Teil weiterhin im Einsatz: ▸ Vorgänger zu SAP ECC unter Nutzung des Client-Server-Modells ▸ R/3 Release 4.7 war die erste Datenbankversion, die auf der SAP-NetWeaver-Plattform basierte und auf jeder Datenbank ausgeführt werden konnte	SAP ECC (ERP Central Component) ist das ERP-Kernprodukt innerhalb der **SAP Business Suite**. Mit SAP ERP 6.0 Enhancement Package 7 führte SAP die erste ERP-Lösung ein, die auf SAP HANA lief.	SAP HANA ist „nur" ein Datenbanksystem und eine Anwendungsentwicklungsplattform. Zentrale Aspekte des SAP HANA Datenbanksystems sind u. a., dass die Daten im Arbeitsspeicher geschrieben werden (**In-memory**) und die Daten **zeilen-** und **spaltenbasiert** abgelegt werden.	S/4HANA ist das neue ERP-System/die neue Business-Suite und wurde speziell für den Betrieb in der HANA-Datenbank geschrieben und kann nicht auf anderen Datenbanken laufen. S/4HANA wurde im Jahr 2015 veröffentlicht. * offiziell ist S/4HANA rechtlich kein Nachfolger einer beliebigen Business Suite, sondern ein neues Produkt.
ON PREMISE	ON PREMISE	ON PREMISE, PRIVATE, PUBLIC & HYBRID CLOUD	ON PREMISE, PRIVATE, PUBLIC & HYBRID CLOUD

Technische Voraussetzungen und Herausforderungen

Für die Konvertierung von SAP R/3 zu SAP S/4HANA gibt es technische Voraussetzungen, die grundsätzlich einzuhalten sind bzw. geschaffen werden müssen. Diese stellen sich wie folgt dar:

- SAP ERP Release 6.0 mit Enhancement Package 7 oder höher
- SAP NetWeaver 7.50 oder höher
- SAP Solution Manager 7.2 oder höher
- Unicode-System
- Single Stack mit nur einer (1) ABAP-Laufzeitumgebung bei Dual Stack (SAP + Java-Stack): Trennung der Stacks vor Konvertierung
- Einsatz SAP zertifizierte Hardware für das Zielsystem (Liste verfügbar)
- Ausreichend Arbeitsspeicher (RAM) für die übernehmende Datenbank
  - Memory Sizing Report durchführen, Altdaten archivieren soweit möglich
  - Achtung: Ausreichend Reserven für die Zukunft einplanen – HANA ist eine In-Memory Datenbank

Gerade in Zeiten von Big Data spielt die Geschwindigkeit der Datenverarbeitung eine entscheidende Rolle. Mit der HANA In-Memory-Datenbank ist durch die Ablage im Hauptspeicher nun eine Echtzeitdatenverarbeitung möglich. Doch vor der Einführung müssen verschiedene Kernaspekte berücksichtigt werden. Zunächst müssen die technischen Voraussetzungen vorliegen. Die neuen SAP-Lösungen wie S/4HANA, C/4HANA, BW/4HANA und Business By Design laufen nativ auf SAP HANA, jedoch sind nicht alle Releases HANA-fähig. Hier muss eventuell noch ausreichend Zeit für einen Releasewechsel eingeplant werden.

Um den Migrationsprozess zu vereinfachen, wird empfohlen, bislang verwendete individuelle Anpassungen und Eigenentwicklungen in SAP zu korrigieren. Bei der neuen In-Memory-Datenbank handelt es sich um eine spaltenorientierte Datenbank, im Altsystem liegt eine Zeilenorientierung vor. Im Zuge der Migration müssen daher über 100.000 Tabellen umgestellt werden.

Notwendige Schritte vor der Konvertierung

Aus Sicht des Wirtschaftsprüfers sind vor der Konvertierung unbedingt folgende Schritte abzuarbeiten:

- Jahresabschluss, Buchungsstopp
  - Saldenvorträge, Jahresabschlüsse, Berichte
- Prüfung der Voraussetzungen mithilfe des Tool Maintenance Planners
- Durchführung SAP S/4HANA Pre-Transition Checks (insb. den sog. Simplification Item Check (SI-Check), der das zentrale Element einer S/4HANA System Conversion darstellt und diese gegen die gesamte Simplification List prüft, was der System Conversion aus technischer Sicht im Weg steht)
- Vorbereitung/Synchronisierung der Geschäftspartner ausgehend von den aktuellen Debitoren und Kreditoren (sofern angebunden). Dies bedeutet insb. eine Überprüfung und Bereinigung der Stammdaten
- Konsistenzprüfung Finanzdaten (Anlagen, Materialwirtschaft, Finance)
- Kompatibilitätsprüfung von Drittanbietersoftware, Eigenprogrammierungen sowie weiteren Abhängigkeiten
  - Mittels der Transaktion ATC (ABAP Test Cockpit) lässt sich eine Code-Überprüfung durchführen, um bspw. Programmierfehler zu erkennen
  - Reduzierung von Non-Standard-Programmen soweit möglich

Wie dargestellt, sind im Vorfeld einer Migration – rein von der technischen Seite gesehen – bereits einige zentrale Punkte zu klären bzw. ggf. das bestehende System soweit anzupassen, dass es migrationsfähig ist. Muss ein Releasewechsel eingeplant werden? Ist mein Release HANA-fähig? Ist eine Korrektur von benutzerdefinierten Code bzw. Eigenprogrammierungen notwendig?

Entscheidend ist und bleibt am Ende weiterhin der Grad der Individualisierung des vorhandenen SAP ERP Systems und Abweichungen in den abgebildeten Geschäftsprozessen vom SAP-Standard, der auch stark beeinflusst, welchen Weg das Unternehmen zur Einführung von SAP S/4HANA wählt. Um den erforderlichen Anpassungsaufwand zu erheben, empfehlen wir vor Beginn des Migrationsprojekts eine Vorstudie durchzuführen. In ergebnisabhängigen Folgeprojekten sollten die ermittelten Themen bearbeitet werden.

Exkurs: Anforderungen aus Prüfersicht

Das Hauptaugenmerk des Prüfers liegt wie bei jeder Migration auf der Prüfung der Vollständigkeit und Richtigkeit der übernommenen Daten. Für die Überprüfung werden Stammdaten, Bewegungsdaten, Verkehrszahlen sowie Anwendungsparameter herangezogen. Der Abgleich erfolgt anhand von Stichproben, durch einen Reportabgleich oder auch durch Transaktionen und Reports. Jedoch zählt nicht nur das richtige Ergebnis, erst durch eine angemessene Dokumentation der Migration kann die Ordnungsmäßigkeit dieser sichergestellt werden. Die Dokumentation ist hier nicht nur ein formeller Akt, sondern ein must-have nach handels- und steuerrechtlichen Vorgaben. Ohne die entsprechende Dokumentation entsteht hier ein Betriebsprüfer-Risiko.

ANSPRECHPARTNER

HAMBURG

Holger Klindtworth
Tel. +49 40 37097-220
holger.klindtworth@ebnerstolz.de

Claudia Stange-Gathmann
CISA, CIA, CISM, QA (DIIR), CDPSE,
ISO/IEC 27001 Lead Auditor
Tel. +49 40 37097-313
claudia.stange@ebnerstolz.de

Ingo Köhne
CISA, CISM, PMP, QAR-IT
Tel. +49 40 37097-315
ingo.koehne@ebnerstolz.de

DÜSSELDORF/KÖLN

Christian Wieder
CISA, CRISC
Tel. +49 211 91332-650
christian.wieder@ebnerstolz.de

FRANKFURT

Sebastian Adam
CISA, ISO/IEC 27001 Lead Implementer
Tel. +49 69 1539249-21
sebastian.adam@ebnerstolz.de

MÜNCHEN

Mark Alexander Butzke
Wirtschaftsprüfer, Steuerberater, CISA, CRISC,
CDPSE, ISO/IEC 27001 Senior Lead Auditor
Tel. +49 89 549018-292
mark.butzke@ebnerstolz.de

Michael Burkhardt
CISA, CRISC,
ISO/IEC 27001 Lead Auditor
Tel. +49 89 549018-293
michael.burkhardt@ebnerstolz.de

STUTTGART

Ralf Körber
Wirtschaftsprüfer, Steuerberater, CISA,
CRISC, CDPSE, Datenschutzbeauftragter
Tel. +49 711 2049-1378
ralf.koerber@ebnerstolz.de

Fabian Diether
CISA
Tel. +49 711 2049-1219
fabian.Diether@ebnerstolz.de

ESECURITY-CERT GMBH

Gerd Niehuis
Lead Auditor ISO 27001 (nativ) / EnWg,
Prüfer § 8a (3) BSIG
Tel. +49 211 540148-01
gerd.niehuis@esecurity-cert.com

Marc Alexander Luge
CISA, CASA, ISO/IEC 27001 Lead Auditor
Tel. +49 211 540148-02
marc.luge@esecurity-cert.com

IMPRESSUM

Herausgeber:
Ebner Stolz GmbH & Co. KG
www.ebnerstolz.de

Ludwig-Erhard-Straße 1, 20459 Hamburg
Tel. +49 40 37097-0

Holzmarkt 1, 50676 Köln
Tel. +49 221 20643-0

Kronenstraße 30, 70174 Stuttgart
Tel. +49 711 2049-0

Redaktion:
Marc Alexander Luge, Tel. +49 211 91332-663
Dr. Ulrike Höreth, Tel. +49 711 2049-1371
novus.it@ebnerstolz.de

Fotonachweis:
Alle Bilder: © www.gettyimages.com