Ausgabe 10, Mai 2019

amendos Spezial:
Outsourcing Teil 3 – Compliance

Eine themenorientierte Zusammenstellung veröffentlichter und unveröffentlichter amendos-Artikel

Cyberkriminalität und Datenskandale häufen sich mittlerweile und führen dazu, dass die Compliance-Anforderungen an Unternehmen stetig wachsen. Gleichzeitig steigt auf Unternehmensseite der Druck diese umzusetzen. Gerade damit tun sich aber viele Unternehmen schwer – wie es jüngst die schleppende Umsetzung der EU-DSGVO zeigte. Angetrieben durch die digitale Transformation lagern Unternehmen zunehmend IT-Services an externe Provider aus, um die technologischen Herausforderungen zu meistern und schnell innovative Lösungen zu schaffen. Die Verantwortung für IT-Sicherheitsrisiken und Compliance-Konformität lässt sich jedoch nicht auslagern. Strafen und Imageschäden treffen weiterhin den Auftraggeber. Der Zwang, IT-Compliance auf Providerverträge und -beziehungen abbilden zu müssen, verstärkt die Notwendigkeit, das Thema „IT-Compliance“ noch strukturierter und effizienter anzugehen. Vor diesem Hintergrund widmen wir uns in dem vorliegenden amendos Spezial mit einer Zusammenstellung neuer und bereits veröffentlichter Artikel verschiedenen Aspekten des Themas „Compliance“.

Inhalt

amendos gmbh
Frankenstraße 3, 20097 Hamburg
www.amendos.de
Tel. +49 (0) 40 / 248 276 00

Effiziente IT-Compliance: In sechs Schritten zum Compliance-Management-System

Die IT dient zum einen dazu, den Geschäftsbetrieb sicher, fehlerfrei, effizient und kostengünstig zu unterstützen. Zum anderen verbessert sie im Zuge der digitalen Transformation die Position des Unternehmens im Wettbewerb und wird zu einem wesentlichen Teil des Kerngeschäftsmodells. Allerdings steigen mit immer schnelleren Innovationszyklen der Technologien und immer komplexeren IT-Landschaften auch die Gefährdungspotenziale. Die mediale Aufmerksamkeit erringen zwar meist nur die großen Skandale wie der um die NSA, Datenskandale um Millionen gestohlener Datensätze im Darknet und Vorfälle, bei denen namhafte Unternehmen (u.a. Facebook und YouTube) betroffen sind. Es ist jedoch anzunehmen, dass all dies nur die Spitze des Eisbergs ist und IT-Risiken fast unterschiedslos alle Unternehmen treffen.

Die Politik reagiert mit immer neuen und schärferen Gesetzen, die bei der zunehmenden Dynamik und Komplexität nicht immer ausreichend ausformuliert und transparent sind. Das zeigte z. B. das Safe Harbour-Urteil des Europäischen Gerichtshofes in 2015, als sich noch nicht einmal die Datenschutzbeauftragten der einzelnen Bundesländer einig waren, ob Verträge mit amerikanischen Firmen, die auf Safe Harbour basieren, sofort – oder erst nach einer Übergangszeit – ihre Gültigkeit verlieren. Sicher war und ist: Die Strafen können drastisch sein und sind in den letzten Jahren zwecks abschreckender Wirkung deutlich verschärft worden.

Wie können nun Gesetzeskonformität und die Einhaltung externer und interner Vorgaben hergestellt und gleichzeitig der Wertbeitrag und die Performance der IT gesteigert werden?

IT-Compliance im Kontext der Unternehmens-Governance

IT-Compliance stellt sicher, dass die IT alle für das Unternehmen relevanten Gesetze oder von diesen abgeleiteten Rechtsnormen, interne Sicherheitsvorgaben und Regularien nachweislich einhält. Die IT-Compliance ist dabei ein wichtiger Bestandteil der Unternehmens-Compliance, die in die Unternehmens-Governance eingebettet ist und vielfältige organisatorische Schnittstellen und thematische Verflechtungen zu diversen Elementen der IT-Bereitstellung aufweist (siehe Abbildung 1).

Steigende regulatorische Anforderungen erfordern ein Compliance-Management-System

Um der Komplexität und Dynamik im IT-Compliance-Management zu begegnen, bedarf es eines professionell aufgestellten Compliance-Management-Systems (CMS). Dieses umfasst sämtliche im Unternehmen eingesetzte Maßnahmen, Strukturen und Prozesse, um Compliance-Konformität sicherzustellen. Ein CMS in der IT zu installieren ist aufwändig. Dennoch gilt es Folgendes zu beachten: Wird zu wenig oder überhaupt nicht in die Umsetzung der regulatorisch geforderten Maßnahmen investiert, drohen Strafen und Sanktionen bis hin zur persönlichen Haftung des CIO. Weiterhin kann es zu Einschränkungen der Geschäftstätigkeit bis hin zur kompletten Einstellung des Geschäftsbetriebs kommen, weil das Geschäftsmodell den regulatorischen Anforderungen nicht standhält.

Der Nutzen eines CMS sollte somit unbestritten sein:

- Vermeidung von Gesetzesverstößen und strafrechtlichen Sanktionen
- Vermeidung von Imageschäden
- Glaubwürdigkeit des Unternehmens nach innen und außen wird gestärkt; dies stärkt Geschäftsbeziehungen, erhöht die Kreditwürdigkeit und ist vielfach Bedingung für die Zulassung zu Ausschreibungen und als Lieferant für öffentliche Auftraggeber.

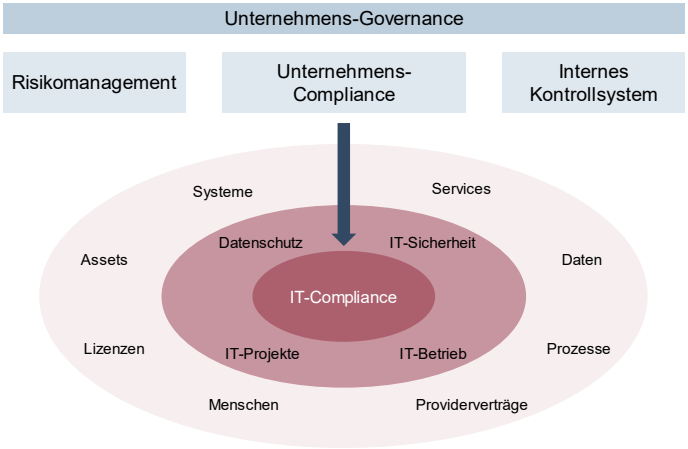


Abbildung 1: Einbettung der IT-Compliance in die Unternehmens-Governance

Kontakt

Was können wir für Sie tun?

Sie haben Fragen oder benötigen Unterstützung bei der Gestaltung Ihres Compliance-Management-Systems?

Treten Sie mit uns in Verbindung.

Wir freuen uns auf Sie!

Tel: +49 (0) 40 / 248 276 00
oder info@amendos.de

- Stärkung der Organisationsstrukturen und der Unternehmenskultur, sodass die Mitarbeiter des Unternehmens unmissverständlich wissen, wie sie sich in bestimmten Situationen Compliance-konform verhalten müssen. Dies steigert nicht nur ihr Vertrauen in das eigene Unternehmen, sondern kann sich auch in der Außenwirkung auf die Kunden fortpflanzen.

In sechs Schritten zum CMS

Ein CMS lässt sich in sechs Schritten einführen:

Schritt 1

Zunächst muss die Geschäftsführung vom Nutzen eines Compliance-Management-Systems überzeugt und sich der Risiken eines fehlenden oder mangelhaften CMS bewusst sein. Die Geschäftsführung muss hinter der Einführung eines CMS stehen. Sie entscheidet über die Implementierung, gibt die Mittel frei und muss das Vorhaben vorantreiben.

Schritt 2

Es müssen gemeinsam Richtlinien für die IT-Compliance erarbeitet, schriftlich fixiert und an alle kommuniziert werden. Dies trägt dazu bei, dass alle Mitarbeiter in der IT diese Richtlinien mittragen – denn sie sind es, die die Richtlinien im Tagesgeschäft mit Leben füllen müssen!

Die Ziele eines CMS müssen allen Beteiligten klar sein:

- Bereits begangene Verstöße gegen die IT-Compliance müssen aufgedeckt und sanktioniert werden.
- Zukünftige Verstöße müssen vermieden werden.

Die Mitarbeiter in der IT müssen auf diese Ziele verpflichtet werden. Um sie einzubinden, empfiehlt es sich daher, nicht nur ein einmaliges Training durchzuführen. Statt dessen gilt es, die fortlaufende Mitarbeit am CMS und an dessen kontinuierlicher Verbesserung zu fördern.

Wenn Teile der IT an externe Provider ausgelagert sind, so ist das CMS auf die Provider und deren Mitarbeiter auszudehnen. Dies muss in den Providerverträgen berücksichtigt sein.

Schritt 3

Ein Compliance-Team muss aufgebaut und organisatorisch verankert werden. In die Zuständigkeit des Compliance-Teams fällt es, dass CMS zu konzeptionieren, im Unternehmen einzuführen, fortlaufend weiterzuentwickeln und an sich verändernde Rahmenbedingungen anzupassen. Das Compliance-Team muss alle erforderlichen Expertisen abdecken:

- Kenntnisse über die aktuell und in der Zukunft im Unternehmen eingesetzten Technologien und deren Risiken unter den Aspekten von Datenschutz und IT-Sicherheit
- juristische Kenntnisse zu den für das Unternehmen relevanten internen und externen Regularien im Kontext der Technologien und Services.

Bei Bedarf müssen für die interdisziplinären Herausforderungen neuer Technologien externe Berater hinzugezogen werden; bestehen Outsourcing-Beziehungen, so sind auch die Provider einzubinden. Für das Team müssen die Aufgaben und Verantwortlichkeiten klar definiert werden. Unternehmensintern müssen alle Mitarbeiter über dieses Compliance-Team informiert und hinsichtlich dessen Aufgabe und Bedeutung für das Unternehmen sensibilisiert werden.

Schritt 4

Die Compliance-Risikobereiche müssen identifiziert werden. Hierzu gehören im Falle eines Outsourcings auch die Risikobereiche auf Seiten der Provider, die ebenfalls erfasst werden müssen.

Dazu bedarf es zunächst einer Übersicht, welche Rechtsnormen für das Unternehmen relevant sind. Das reicht von generell für Unternehmen geltende Regularien (z. B. BGB, HGB) über branchenspezifische (z. B. MaRisk im Finanzbereich) bis hin zu technologiebedingten (z. B. EU-DSGVO im Falle der elektronischen Datenverarbeitung). Hinzu kommen externe Normen (z. B. Dokumente des Instituts der Wirtschaftsprüfer IDW, Frameworks wie ITIL und COBIT, ISO-Normen) und interne Richtlinien (z. B. Organisationshandbuch, Sicherheitsrichtlinien, Betriebshandbuch).

Unternehmensspezifisch muss zusammengestellt werden, welche IT-gestützten Business-Prozesse und IT-Services von diesen Rechtsnormen betroffen sind.

Über diese Zusammenstellung wird eine Risikoanalyse durchgeführt: Welche Risiken gibt es – wie groß ist das Schadenspotenzial infolge fehlender oder mangelhafter Regelkonformität?

Daraus folgt, welche Anforderungen die internen und externen Provider und die internen IT-Bereiche erfüllen müssen. Die notwendigen technischen, organisatorischen, personellen und vertraglichen Maßnahmen dazu müssen erarbeitet und konzeptioniert werden.

Schritt 5

Sind die Maßnahmen identifiziert, gilt es, sie umzusetzen. Das CMS nimmt damit seinen Betrieb auf.

Verstöße gegen das CMS machen Sanktionen erforderlich. Diese müssen auch angewendet werden! Ursachen müssen analysiert und Maßnahmen ergriffen werden, um zukünftige Verstöße zu vermeiden.

Schritt 6

Compliance-Management ist keine Einmal-Aktion: Die Dynamik in Technologien und fortlaufende Anpassungen und Neuerungen in den Regularien machen es erforderlich, kontinuierlich Aktualisierungen vorzunehmen und das System selbst hinsichtlich seiner Wirksamkeit einem kontinuierlichen Verbesserungsprozess zu unterziehen.

Fazit

Wenn ein Unternehmen bei der Implementierung des CMS nach diesen sechs Schritten vorgeht , dann hat es von externen Revisoren (z. B. Wirtschaftsprüfern) wenig zu befürchten. Die sechs Schritte schaffen die notwendige Transparenz, wie das Unternehmen mit dem Thema „IT-Compliance“ umgeht und Verstöße handhabt. So wird IT-Compliance zu einem wertvollen Teil der Unternehmens-Governance, der Risiken minimiert und die Fähigkeit des Unternehmens steigert, Potenziale aus neuen Technologien zu schöpfen und durch besseren Service oder mehr Innovation seine Wettbewerbsposition zu stärken.

Michael Schneegans, Jörg Bujotzek

Von der Corporate Governance zur IT-Compliance

Corporate Governance und IT-Compliance sind unscheinbare Begriffe aus dem Business Umfeld, mit deren Definitionen und Interpretationen sich dennoch unzählige Diskussionsseiten im Internet befassen. Es wird gewissermaßen mehr Energie darauf verwendet, die Definition zu perfektionieren als deren inhaltlichen Belangen konsequent nachzugehen. Dieser Artikel soll anhand eines Beispiels die Bedeutung und den Zusammenhang einfach veranschaulichen.

Der Begriff Compliance ist laut Duden mit vier verschiedenen Bedeutungen belegt. Die wohl zutreffendste im IT-Zusammenhang ist „(Wirtschaftsjargon) regelgerechtes, vorschriftsgemäßes, ethisch korrektes Verhalten“. Der Begriff Corporate Governance hingegen taucht gar nicht erst im offiziellen deutschen Sprachschatz auf. Wörtlich übersetzt würde er Unternehmensregierung bedeuten. Man kann ihn aber eher mit Regeln der „guten“ Unternehmensführung gleichsetzen.

Was verbirgt sich hinter diesen Regeln und was ist das eigentliche Ziel, welches damit verfolgt wird? Im Kern geht es zunächst um „gesunden Menschenverstand“ in der Unternehmensführung und ein ausgewogenes Maß in der Adressierung betriebswirtschaftlicher und gesellschaftlicher Anforderungen.

Braucht es nun aber eine Regierung oder Behörde um dieses Maß zu finden? Betrachtet man z.B. den Hintergrund des in Europa eingeführten und den nationalen Gegebenheiten angepassten Deutschen Corporate Governance Kodex, so wird schnell deutlich, dass hiermit auch andere Ziele anvisiert werden. Investoren soll vermittelt werden, dass hier ansässige Aktiengesellschaften eine Unternehmensführung besitzen, die für eine angemessene Transparenz und Investitionssicherheit Sorge trägt. Dieses Beispiel zeigt, dass es durchaus unterschiedliche Auslegungen des Konzeptes „Corporate Govenance“ gibt: Während einige Unternehmen darin eher ein Marketinginstrument sehen, verstehen es andere als Regelwerk zur Verbesserung des gesellschaftlichen und nachhaltigen Miteinanders. Es existiert sogar eigens eine Regierungskommission um diesen Kodex zu überwachen.

Ist so viel Aufwand wirklich nötig um etwas zu regulieren, was es schon immer gab? Offensichtlich – ja. Die Globalisierung sowie die extrem schnelllebigen Märkte zwingen Unternehmen, dieses Thema strukturierter und vielleicht auch regulierter als noch vor 50 Jahren anzugehen. Ein Unternehmen steht heutzutage mehr denn je im Fokus der Öffentlichkeit. Nachrichten über ethisch fragwürdige oder nachlässige Geschäftspraktiken wie z.B. die Bezahlung von Niedriglöhnen oder Datenpannen verbreiten sich binnen Minuten im Internet und können ein Unternehmen massiv in Bedrängnis bringen. Eine Corporate Governance soll solche und weitere Risiken minimieren, indem zuerst das Umfeld analysiert und auf Basis der Ergebnisse Regelungen definiert werden, um in diesem zu bestehen.

Eine Corporate Governance wird maßgeblich geprägt durch drei Themenfelder: die rechtlichen nationalen und internationalen Regelungen, die betriebswirtschaftlichen und strategischen Ziele sowie gesellschaftliche Rahmenparameter. Erst nachdem dieses komplexe Umfeld erfasst, analysiert und eine Corporate Governance aufgestellt wurde, kann daraus auch eine ganzheitliche IT-Governance abgeleitet werden. In dieser ist beschrieben wie die IT die Unternehmensstrategie unterstützen und Unternehmenswerte schützen soll. Die IT-Compliance ist ein wesentlicher

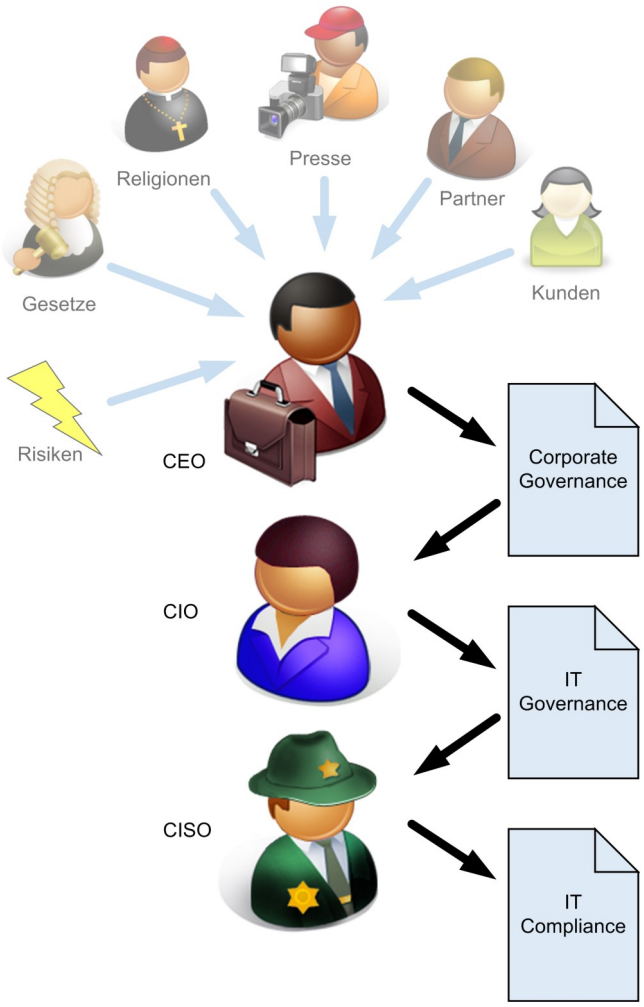


Abbildung 1: Von der Corporate Governance zur IT-Compliance

Bestandteil der IT-Governance. Sie stellt sicher, dass die IT „compliant“ gegenüber den in der Corporate Governance identifizierten Regeln agiert und implementiert angemessene Maßnahmen, um die Unternehmenswerte zu schützen. Um den Schutzbedarf zu quantifizieren, bedarf es eines soliden Risikomanagements, das die Gefahren, denen die Werte unterliegen, analysiert und entsprechende Maßnahmen ableitet. Danach existiert eine Basis um IT-Compliance auch bewertbar zu machen. Ohne diese Voraussetzung ist es nicht möglich einzuschätzen, ob Aufwendungen, z.B. zur Einhaltung von gesetzlichen Vorgaben, verhältnismäßig und ausreichend sind.

Die IT-Compliance hat als Antriebsmotor die Ergebnisse der Risikoanalyse und befasst sich damit, angemessene und adäquate Mechanismen zu implementieren, um die geplanten Maßnahmen umzusetzen. Folgendes sehr vereinfachtes Beispiel soll diesen Entstehungsprozess für eine einzelne Maßnahme veranschaulichen.

Ein internationaler IT-Konzern, der u.a. auch Cloud-Dienste anbietet, überarbeitet seine Corporate Governance und überprüft, ob sie noch der heutigen Marksituation gerecht wird. Dabei wird festgestellt, dass durch die andauernde öffentliche Diskussion über Spionagefälle das Misstrauen der deutschen Kunden gegenüber der Informationstechnologie extrem gestiegen ist. Insbesondere die Speicherung sensibler personenbezogener Daten im amerikanischen Raum wird von vielen deutschen Kunden als nicht mehr tragbares Risiko gesehen. Auch die zu jenem Zeitpunkt gültigen Abkommen wie Safe-Harbor, die sicherstellen sollten, dass auch in den USA für diese Daten nationale Datenschutzbestimmungen gelten, ändern daran nichts. Diese basieren auf einer freiwilligen Verpflichtung der dortigen Anbieter und können durch amerikanische Gesetze wieder ausgehebelt werden.

Das Unternehmen ist aus betriebswirtschaftlicher Sicht natürlich daran interessiert, sich am Markt zu behaupten. Deshalb muss auf den aktuellen gesellschaftlichen Wandel in Bezug auf die steigende Skepsis reagiert werden. Die deutsche Gesetzgebung verschärft diese Situation zusätzlich, indem z.B. die Speicherung steuerlich relevanter Daten ausschließlich im EU Wirtschaftsraum und auch nur nach vorheriger Genehmigung der Finanzbehörden erfolgen darf. Hier zeichnet sich ein konkretes Risiko ab: die entsprechende Kundengruppe wird weniger oder gar keine der angebotenen Cloud Lösungen mehr nutzen. In die überarbeitete Corporate Governance wird nun aufgenommen, sich nationalen Anforderungen im IT-Sicherheitsumfeld intensiver zu widmen. Es sollen transparente Lösungen geschaffen werden, die das Unternehmen so am Markt etablieren, dass es sich im IT-Sicherheitsumfeld von der Konkurrenz positiv abhebt. Als Maßnahme wurde definiert, die rechtlichen und technischen Gegebenheiten des eigenen Serviceangebots daraufhin anzupassen.

Der erste Schritt ist, eine deutsche GmbH auszugründen, die damit für Kunden eindeutig sichtbar dem deutschen Recht unterliegt. Der vermeintliche sichere Anbieter würde aber schnell an Akzeptanz verlieren, wenn sich herausstellt, dass die Daten im Rechenzentrum des amerikanischen Mutterkonzerns liegen. Weshalb auch noch eine zweite, technische Maßnahme von Nöten ist: die Schaffung nationaler Rechenzentren. Nun ist es aber für dieses vergleichbar kleine Unternehmen nicht möglich, eine mit dem Mutterkonzern vergleichbare komplette Betriebsorganisation zu stellen. Die favorisierte Lösung in diesem Fall ist das Outsourcing der betreffenden Leistungen. Entscheidend ist jetzt, dass die eingekauften Dienste neben den typischen Faktoren wie Verfügbarkeit, Kosten usw. vor allem eine Anforderung erfüllen: eine nachweislich ausnahmslose Speicherung der Daten auf deutschem Bundesgebiet.

Diese kleine Nuance ist aus technischer und rechtlicher Sicht nicht zwingend erforderlich. Aber dadurch, dass diese Anforderung in der Corporate Governance begründet ist, wird sie entscheidend, um „compliant“ zu sein.

Feedback

Ihre Meinung zählt!

Sie haben Fragen, Anmerkungen oder Verbesserungsvorschläge?

Treten Sie mit uns in Verbindung. Wir freuen uns auf Ihr Feedback!

info@amendos.de

Fazit:

Im IT Jargon werden immer wieder neue Begriffe Einzug halten, (IT-) Governance und (IT-) Compliance sind aber bereits feste Bestandteile. Entscheidend für den Umgang mit den dahinterstehenden Konzepten ist jedoch nicht, die treffendste Definition der beiden Begriffe zu kennen, sondern die dahinterstehenden Werte und Ziele zu leben. Jedes etablierte Unternehmen hat eine mehr oder weniger umfangreich definierte Corporate Governance, ob sie nun auch so benannt ist oder nicht. Ein Verantwortlicher im IT Umfeld sollte daher immer im Auge behalten, ob die von ihm verantwortete IT-Compliance auch wirklich alle Anforderungen der aus der Unternehmensstrategie abgeleiteten Corporate Governance optimal und präzise unterstützt.

Henry Wudi

Compliance-Risiken beim IT-Outsourcing minimieren

Compliance rückt in der IT oft erst ins Blickfeld, wenn spektakuläre, medienwirksame Ereignisse wie das EuGH-Urteil zu Safe Harbour vom Oktober letzten Jahres eintreten – oder eine Revision, z. B. durch Wirtschaftsprüfer, bereits im Hause ist. Letzteres führt dann zu hektischen Reaktionen und, wenn die Revisoren Kritikpunkte identifiziert haben, zu erheblichen Anstrengungen, Versäumtes nachzuholen. Kritisch wird es insbesondere beim Outsourcing, wenn die externen Provider in das Procedere eingebunden werden müssen und das beauftragende Unternehmen aus eigener Kraft allein die Gesetzeskonformität nicht herstellen kann. Wir stellen die wesentlichen vorbeugenden Schritte zusammen, damit solche Situationen gar nicht erst auftreten.

Selbst ein – vermeintlich – einfaches Vorhaben, wie z.B. die Office-Programme des IT-Providers Microsoft zukünftig aus der Cloud zu beziehen, birgt bereits Sprengstoff. Von den Nutzern dieser Programme wird dann schnell auch die Speicherung von Office-Dokumenten, also Daten, in der Cloud gewünscht. Das kann mit wenigen Handgriffen umgesetzt werden, schafft aber unter Compliance-Aspekten eine völlig neue Situation. Spätestens dann, wenn Daten ins Spiel kommen, sind sorgfältige Compliance-Betrachtungen erforderlich.

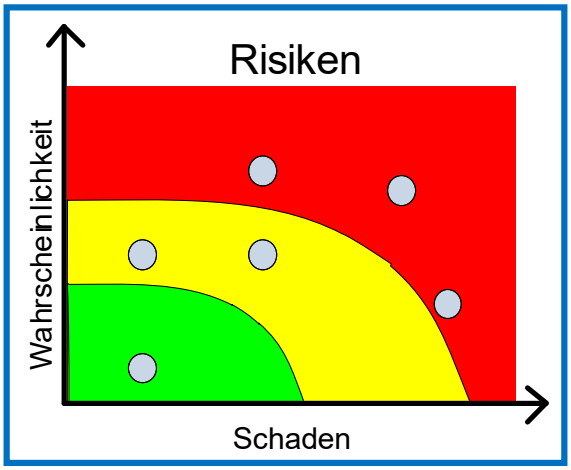
Rechtlichen Rahmen abstecken

Eingehalten werden müssen z. B. die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) bei rechnungslegungsrelevanten oder das Bundesdatenschutzgesetz (BDSG) bei personenbezogenen Daten, für nicht in der DSGVO geregelte Bereiche. Hinzukommen können internationale Regelungen, z. B. die unmittelbar geltende EU-Datenschutz-Grundverordnung (DSGVO), branchenspezifische, z. B. die MaRisk (BA) bzw. MaRisk (VA) für Banken und Versicherungen, und Normen und Standards wie ISO/IEC 27001, ISO/IEC 27018 und die Cloud-Standards des National Institute of Standards and Technology. Es ist somit unerlässlich, die für das auslagernde Unternehmen zu beachtenden Regularien zusammenzustellen.

Die grundlegenden Erwartungen von Wirtschaftsprüfern bei einer Revision sind in der IDW RS FAIT 5 des Instituts der Wirtschaftsprüfer in Deutschland e. V., Fachausschuss für Informationstechnologie (FAIT), festgeschrieben:

> Bei allen Arten des Outsourcings und damit auch beim Cloud Computing verbleibt die Verantwortung für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen bei den gesetzlichen Vertretern des auslagernden Unternehmens. Aus diesem Grund müssen die gesetzlichen Vertreter die aus dem Outsourcing entstehenden Risiken und die damit verbundenen Auswirkungen […] beachten. (IDW RS FAIT 5; www.idw.de)

Hieraus folgt die Notwendigkeit einer Risikoanalyse: Da sich die IDW RS FAIT 5 aus mehr als hundert Unterpunkten zusammensetzt, folgt eine Vielzahl an Risiken, die es aus Compliance-Sicht zu adressieren gilt.



Risikoarten des IT-Betriebs:

- Kaufmännische Risiken
- Rechtliche Risiken (Compliance)
- Technische Risiken
- Organisatorische Risiken
- Ressourcen-Risiken
- Termin-Risiken

Abbildung 1: Risikoanalyse für den IT Betrieb

Es empfiehlt sich, die aus den gesetzlichen Anforderungen resultierenden Risiken frühzeitig zu identifizieren und die abgeleiteten Erkenntnisse zu berücksichtigen. Schon bei der Evaluierung von Pro und Contra eines Outsourcings muss klar sein, welche Risiken eintreten können – und ob sie beherrschbar sind. Die abgeleiteten Maßnahmen müssen dann in die Konzeption des Outsourcing-Vorhabens einfließen, diktieren wesentliche Kriterien für die Auswahl des Providers und sind schließlich Bestandteil des abzuschließenden Vertrages.

Risiken analysieren

Ein traditionelles Verfahren im Risikomanagement ist, die Risiken möglichst vollständig zu identifizieren und anhand von Eintrittswahrscheinlichkeiten und Auswirkungen zu bewerten. Die Ermittlung erfolgt z. B. im Rahmen eines Expertenworkshops. Identifizierte Risiken können nach Risikoarten gruppiert werden. Für jedes Risiko sind Maßnahmen zu definieren, wie mit ihnen umzugehen ist. (Eine Orientierung zur Risikoanalyse bietet u. a. die ISO 31000, Risk Management – Principles and Guidelines.)

Wichtiger Hinweis:
Wenn beim Outsourcing hinsichtlich der Compliance-Verpflichtungen des beauftragenden Unternehmens die Aufgaben und Mitwirkungspflichten des Providers im Vertrag nur unzureichend geregelt sind, dann können Nachbesserungsforderungen von Revisoren gewaltige Schwierigkeiten und Kosten für den Auftraggeber verursachen.

Risiken den Vertragspartnern zuweisen

Beim Outsourcing verteilen sich die Risiken auf den Auftraggeber und den Provider. Die folgende Gruppierung der Risiken (aus der Sicht des Auftraggebers) liefert einen Überblick, wer in welcher Form für das Risiko zuständig ist:

- Auftraggeberrisiken (verbleiben beim auslagernden Unternehmen),
- Providerrisiken (werden auf den Provider übertragen),
- Schnittstellenrisiken (technisch / organisatorisch)

So lässt sich auch schnell erkennen, was

- bereits bei einer **Entscheidung** für oder gegen das Outsourcing abzuwägen ist,
- als **Auswahlkriterium** bei der Providerwahl dient,
- im **Providervertrag** klar und eindeutig definiert werden muss,
- und im späteren **Betrieb** vom Providermanagement auf Seite des Auftraggebers zu tun ist.

Wichtiger Hinweis:
Beim Outsourcing verbleibt die Compliance-Verantwortung beim Auftraggeber und kann nicht an den Provider abgegeben werden. Entsprechende Aufgaben des Risikomanagements müssen deshalb im Auftrag gebenden Unternehmen verbleiben und können dort z. B. im Providermanagement verankert werden

Tabelle 1 auf der nächsten Seite zeigt für die Risikoarten die wesentlichen Aspekte dieser Betrachtung und konkretisiert die zu ergreifenden Maßnahmen.

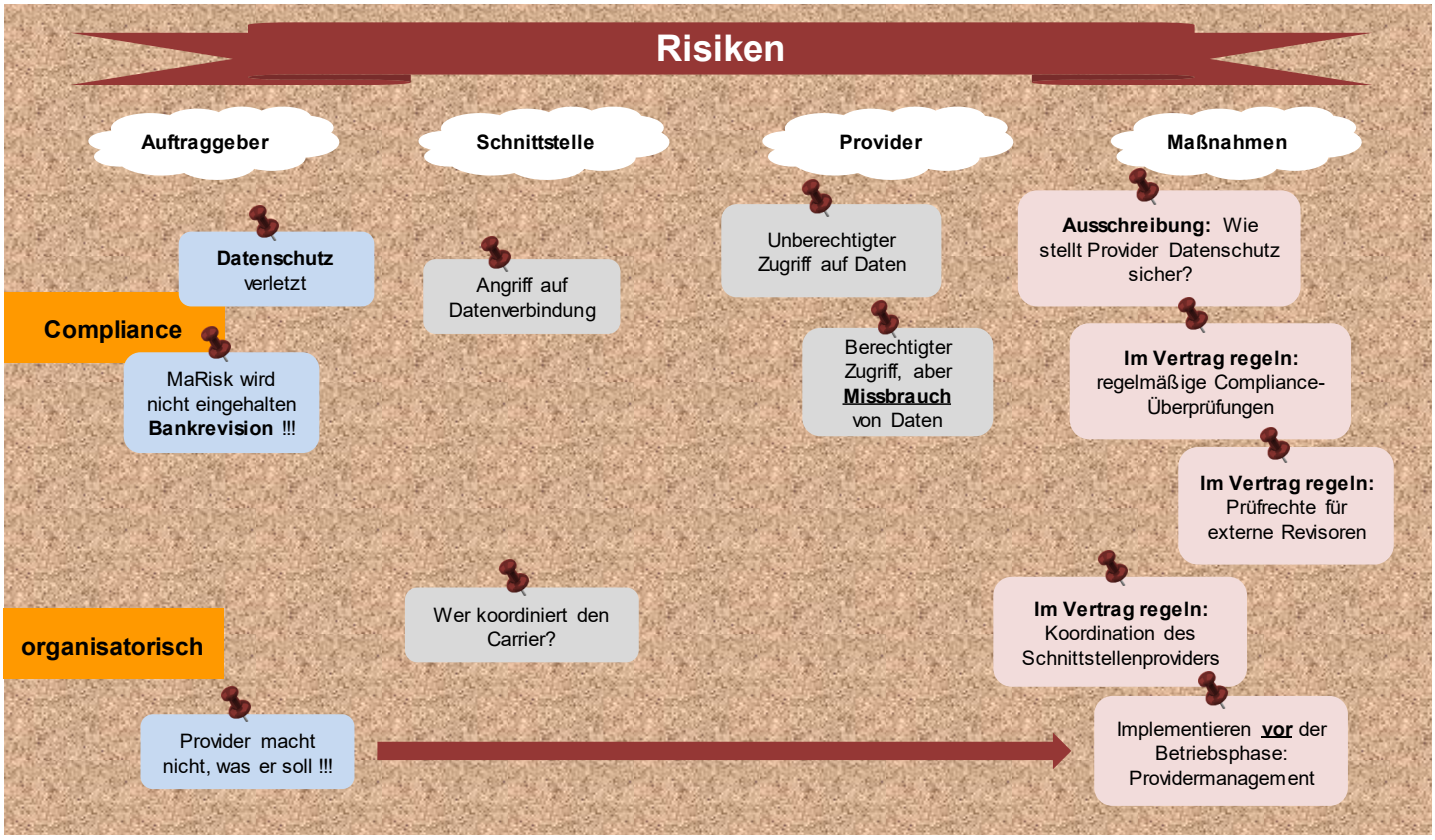


Abbildung 2: Auftraggeber-, Schnittstellen- und Providerrisiken und abgeleitete Maßnahmen

Risikoart	Auftraggeber	Schnittstelle	Provider	Maßnahmen
Kaufmännische Risiken	- Bleibt für die Wirtschaftlichkeit des IT-Betriebs verantwortlich. - Bleibt verantwortlich für wirtschaftliche Misserfolge, Imageschäden etc., auch wenn der Provider sie verursacht hat. - Wirtschaftliche Probleme des Providers sind aus Sicht des Auftraggebers ein Risiko.	Zu berücksichtigende Kostenposition im Business Case (z. B. die Kosten für die Einrichtung und den Betrieb einer Datenverbindung zwischen dem Unternehmen und dem Provider).	- Verantwortlich nur für die eigenen kaufmännischen Risiken. - Verantwortlich für die vertragsgemäße Erbringung der IT-Services, aber **nicht** für die kaufmännischen Risiken des Auftraggebers. - Aus Sicht des Unternehmens dann relevant, wenn der Provider seine vertraglich vereinbarten Leistungen aufgrund wirtschaftlicher Probleme nicht mehr erfüllt.	- Berücksichtigung der kaufmännischen Risiken und insbesondere deren Folgen bei Eintritt schon bei der Auswahl des Providers. - Aufnahme der Kosten für die Schnittstelle in die Evaluierung des Outsourcing-Vorhabens. - Aufnahme von Regelungen im Providervertrag für den Fall, dass der Provider wirtschaftliche Probleme hat. - Implementierung eines Prozesses der regelmäßigen Risikoüberwachung durch das Providermanagement und Maßnahmen zur Schadensbegrenzung, wenn der Risikofall eintritt.
Rechtliche Risiken (Compliance)	Bleibt verantwortlich für die Einhaltung von Gesetzen bei Vertragsabschluss **und** während der Vertragslaufzeit (letzteres relevant insbesondere bei zukünftigen Gesetzesänderungen).	- Neue Risikoquelle, insbesondere relevant für Datensicherheit und Datenschutz, wenn Daten über diese Schnittstelle übertragen werden. - Wird die Schnittstelle durch einen weiteren Provider zur Verfügung gestellt (bei physikalischen oder drahtlosen Datenverbindungen i. d. R. gegeben), so ist dieser Provider gesondert unter Risiko- und Compliance-Aspekten zu betrachten.	-Stellt den IT-Service dem Unternehmen vertragsgemäß zur Nutzung zur Verfügung. - Ist über den Vertrag hinaus nicht verpflichtet, weitere Vorkehrungen zu treffen, um Compliance-Konformität sicherzustellen (sofern kein offensichtlicher grober Gesetzesverstoß vorliegt). - Übernimmt nicht die Verpflichtung zur Compliance-Konformität (im Falle einer Revision).	- Bewertung des Providers auf Compliance-Konformität schon bei der Auswahl vor Vertragsabschluss. - Regelungen, wie die Compliance-Konformität regelmäßig überprüft wird (Vorlage von Zertifizierungen, Kontrollrechte für Externe, z. B. Wirtschaftsprüfer, Revisoren). - Regelungen im Providervertrag über die Mitwirkungspflichten bei einer Revision (z. B. Vorlage von Dokumentationen, Zutrittsrechte für Revisoren). - Regelungen im Providervertrag hinsichtlich potenzieller, zukünftiger Gesetzesänderungen.
Technische Risiken	Werden für die outgesourcten IT-Services auf den Provider verlagert. **Achtung:** Wenn der Provider diese Risiken nicht beherrscht, dann wird das Unternehmen dennoch die Konsequenzen tragen müssen (Image-/Umsatzverlust; Folgen aus Compliance-Verstößen).	Kommen neu hinzu; es ist zu regeln, wer die Risiken trägt, d. h., wer für die technische Einrichtung und Administration der Schnittstelle zuständig ist.	Stellt die technische Infrastruktur für die outgesourcten IT-Services zur Verfügung und übernimmt dabei die entsprechenden Risiken gemäß Providervertrag.	- Es ist im Vertrag genau festzulegen, welche technischen Komponenten die outgesourcten IT-Services umfassen. - Dies gilt auch und insbesondere für die Schnittstellenkomponenten. - Wird die Schnittstelle durch einen weiteren Provider bereitgestellt, so sind auch die daraus resultierenden Aspekte vertraglich zu berücksichtigen (ggf. auch in dem Vertrag mit dem weiteren Provider).
Organisatorische Risiken	Werden für die outgesourcten IT-Services auf den Provider verlagert. **Wichtig:** Es liegt in der organisatorischen Verantwortung des Unternehmens, ein adäquates Providermanagement zu implementieren, das neben der Steuerung des Providers im Regelbetrieb auch die regelmäßige Prüfung der fortlaufenden Compliance-Konformität des Providers nachhält.	Ist organisatorisch neu zu planen; z. B. - Implementierung eines Providermanagements im Unternehmen, das die organisatorische Schnittstelle zum Provider bildet. - Festlegung von Verantwortlichkeiten. - (Neu-)Design der Betriebsprozesse (Incidents, Service Request, Changes, Events, Problems, …). - Wird die Schnittstelle durch einen weiteren Provider zur Verfügung gestellt, so ist dies zu berücksichtigen.	Stellt die (Aufbau-/Ablauf-) Organisation für den Betrieb der IT-Services und übernimmt dabei die entsprechenden Risiken gemäß Providervertrag.	Im Vertrag genau festzulegen: - Organisatorische Aufgaben und Pflichten des Providers, z. B. Organisation von Zugriffsrechten. - Aufgaben und Rechte des Providermanagements gegenüber dem Provider, z. B. Einsichtnahme in Organisationshandbuch des Providers und Zugriffsprotokolle. - Neue Betriebsprozesse sind vor Inbetriebnahme zu planen, vertraglich zu fixieren und zu implementieren.
Ressourcen-Risiken	Werden für die outgesourcten IT-Services auf den Provider verlagert. **Achtung:** Je nach Inhalt des Provideraufrags kann der Aufwand des Providermanagements im Betrieb hoch sein, sodass entsprechende Ressourcen seitens des Unternehmens eingeplant und vorgehalten werden müssen. Dies gilt auch für die Unterstützung des Providers bei der Transition der IT-Services und im Regelbetrieb.	- Kann insbesondere relevant sein bei der erstmaligen Einrichtung der Schnittstelle. - Wird die Schnittstelle durch einen weiteren Provider zur Verfügung gestellt, so sind auch dessen Ressourcen und die (erhöhten) Aufwände für die Koordination zu berücksichtigen.	Stellt die benötigten personellen Ressourcen für die outgesourcten IT-Services zur Verfügung und übernimmt dabei die entsprechenden Risiken gemäß Providervertrag.	Im Providervertrag i. d. R. durch Service Level Agreements zu regeln (Reaktionszeiten bei Störungen, zeitliche Verfügbarkeit von Mitarbeitern des Providers, …). **Wichtig:** Schon bei Vertragsschluss sollte daran gedacht werden, dass irgendwann der Vertrag nicht mehr fortgesetzt wird und die IT-Services z. B. an einen anderen Provider übergeben werden sollen. Der (noch) aktive Provider muss bei einem solchen Übergang die notwendigen Ressourcen zur Unterstützung bereithalten.
Termin-Risiken	Werden für die outgesourcten IT-Services auf den Provider verlagert.	- Insbesondere relevant bei der erstmaligen Einrichtung der Schnittstelle. - Wird die Schnittstelle durch einen weiteren Provider zur Verfügung gestellt, so sind Termine entsprechend über mehrere Parteien zu koordinieren und ggf. die erhöhten Koordinationsaufwände zu berücksichtigen.	Muss termingerecht seine vertraglichen Verpflichtungen erfüllen und trägt die daraus resultierenden Risiken.	Im Vertrag ist zu regeln, wie mit Terminverfehlungen des Providers umzugehen ist (z. B. eine Malus-Regelung).

Tabelle 1: Risiken und Maßnahmen

Komplexe Situationen beherrschen

Der beschriebene Ansatz kann auch in komplexeren Situationen angewendet werden:

- Der Provider bietet mehr als einen IT-Service. Dies ist im eingangs erwähnten Beispiel von Microsofts Office 365 der Fall. Ein Service ist die reine Bereitstellung der Office-Applikationen aus der Cloud, ein anderer die Speicherung der Dokumente – nicht mehr in der Infrastruktur des Auftraggebers, sondern in der des Providers! Je Service ist eine separate Risikoanalyse zu erstellen, denn die beiden Services sind unter Compliance-Aspekten völlig unterschiedlich zu bewerten.
- Das Unternehmen hat mehr als einen Provider beauftragt (Multi-Provider-Umgebung). In diesem Fall ist je Provider eine Risikoanalyse durchzuführen. Interagieren einzelne Provider auch untereinander, so sind deren Schnittstellen zusätzlich zu betrachten.

Diese Fälle werden wir in einem unserer folgenden Newsletter noch genauer betrachten.

Lesen Sie hierzu auch:

amendos Spezial: Outsourcing Teil 2 – Providerwechsel

Fazit

Compliance muss beim Outsourcing an einen IT-Provider kein „Schreckgespenst“ sein. Es gilt aber, auf Basis der Kenntnis relevanter rechtlicher Regularien eine sorgfältige Risikoanalyse durchzuführen. Je Risiko muss eindeutig definiert sein, welche von den Vertragsparteien dabei welche Verpflichtungen hat. Dies muss schon bei der Auswahl des Providers berücksichtigt, im Vertrag fixiert und im Regelbetrieb fortlaufend nachgehalten werden. Die Verantwortung für die Compliance-Konformität verbleibt immer beim Auftraggeber; das Risikomanagement kann deshalb nicht allein dem Provider überlassen werden.

Michael Schneegans

amendos
Karriere-Know-how

Seminare zum Thema IT-Providerwechsel

Outsourcing

Seminar „IT-Outsourcing – Konzeption, Angebotseinholung und Vergabe, Transition“

In diesem Seminar erlernen Sie…

- die Erstellung eines Konzepts, dass die Spezifikation der externen Leistungen, Schnittstellen zur internen Organisation und Maßnahmen zur Providersteuerung inklusive der Sicherstellung der Compliance umfasst,
- die Gestaltung eines Request-for-Proposal-Verfahrens, das die Auswahl des „richtigen“ Providers und eine solide Vertragsgrundlage sicherstellt,
- die Sicherstellung einer reibungslosen Transition.

Termin: 04.11. - 05.11.2019 in Hamburg

Providermanagement

Grundlagen IT-Providermanagement – Steuerung externer IT-Provider in der Betriebsphase

In diesem Seminar erlernen Sie…

- die 9 Dimensionen, die einem effizienten Providermanagement zugrunde liegen,
- welche Rahmenvorgaben, Methoden und Organisation für eine erfolgreiche Zusammenarbeit notwendig sind,
- wie ein Compliance-Management in der Betriebsphase ausgestaltet sein sollte und
- wie der Providermanager in das Compliance-Management-System eingebunden wird.

Termin: 03.06. - 04.06.2019 in Hamburg

Providerwechsel

IT-Providerwechsel – Erfolgreicher Austausch des Providers beim IT-Outsourcing

In diesem Seminar erlernen Sie…

- welche Key Success Factors für eine reibungslose Transition zu einem neuen Provider relevant sind,
- welche Voraussetzungen hierfür zu schaffen sind,
- die Erarbeitung einer Exit-Strategie, die Risiken minimiert und Compliance-konform ist,
- welche Maßnahmen zielführend sind und den optimalen Nutzen schaffen.

Termin: 23.09.2019 in Hamburg

Wir beraten Sie gerne: Tel +49 (0) 40 / 248 276-00, Fax +49 (0)40) / 248 276-01, www.amendos.de, info@amendos.de

DSGVO-Umsetzung – mit Fokus auf IT-Outsourcing

Seit 25. Mai 2018 gilt in Deutschland die Datenschutz-Grundverordnung (DSGVO). Jüngste Studien zeigen aber, dass sich hinsichtlich ihrer Umsetzung in den meisten Unternehmen noch viel zu wenig getan hat (siehe z. B. Bitkom, *Kaum Fortschritt bei der Umsetzung der Datenschutz-Grundverordnung*[1]). Gerade in Unternehmen mit Multi-Providerumgebung haben sich die Herausforderungen jedoch potenziert. Wir wollen deshalb dieses Thema noch einmal aufgreifen und bezüglich IT-Outsourcing den „roten Faden" skizzieren, was von wem zu tun ist.

DSGVO und IT-Outsourcing

Die DSGVO[2] umfasst 11 Kapitel mit insgesamt 99 Artikeln und einer Vielzahl von Absätzen (zur besseren Orientierung siehe die nachfolgende Tabelle). Sie unterscheidet zwischen dem Verantwortlichen (Auftraggeber) und dem Auftragsverarbeiter (Provider im Falle eines Outsourcings). Die Aufgabenverteilung ist im Wesentlichen in Kapitel IV geregelt.

Kapitel		Artikel
I	Allgemeine Bestimmungen	1 – 4
II	Grundsätze	5 – 11
III	Rechte der betroffenen Person	12 – 23
IV	Verantwortlicher und Auftragsverarbeiter	24 – 43
V	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	44 – 50
VI	Unabhängige Aufsichtsbehörden	51 – 59
VII	Zusammenarbeit und Kohärenz	60 – 76
VIII	Rechtsbehelfe, Haftung und Sanktionen	77 – 84
IX	Vorschriften für besondere Verarbeitungssituationen	85 – 91
X	Delegierte Rechtsakte und Durchführungsrechtsakte	92 – 93
XI	Schlussbestimmungen	94 – 99

Tabelle1: Gliederung der DSGVO

Betroffen sind alle Outsourcing-Aktivitäten, bei denen personenbezogene Daten – definiert in Kapitel I der DSGVO – im Spiel sind. Wir zeigen die notwenigen Schritte auf, mit denen der Auftraggeber seine Providerbeziehungen auf einen DSGVO-konformen Stand bringt.

Verzeichnis aller Verarbeitungstätigkeiten erstellen

In Kapitel IV, Art. 30, fordert die DSGVO, dass der Auftraggeber ein vollständiges Verzeichnis aller Verarbeitungstätigkeiten personenbezogener Daten führen muss. Hier werden auch die externen Provider vermerkt, wenn sie innerhalb einer Tätigkeit Zugang zu Daten bekommen und sie verarbeiten. Dieses Verzeichnis bildet den Ausgangspunkt für alle weiteren Betrachtungen. (Nicht zu vergessen: Auch die Daten der verschiedenen Ansprechpartner auf Seite der Provider sind personenbezogen und müssen gleichermaßen betrachtet werden.)

Risikoanalyse durchführen

Jede Datenverarbeitungstätigkeit sollte der Auftraggeber einer Risikoanalyse hinsichtlich des Datenschutzes unterziehen, wie wir es z. B. in unserem Newsletter 1/2016 beschrieben haben. (In bestimmten Fällen ist sogar zwingend eine Datenschutz-Folgeabschätzung durchzuführen; vgl. Kapitel IV, Art. 35).

Maßnahmen ableiten

Aus der Risikoanalyse lassen sich die Technischen und Organisatorischen Maßnahmen (TOM) ableiten, um Risiken zu minimieren und sich so DSGVO-konform aufzustellen. Die DSGVO bleibt in Art. 32 zur Ausgestaltung eher vage: „(1) Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, […]". Konkretere Hinweise findet man z. B. auf über 70 Seiten in der *Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen* des Bundesverbandes IT-Sicherheit[3] und weiteren Quellen zur IT-Sicherheit.

Die TOM sind je Verarbeitungstätigkeit zu definieren und im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Daraus ergibt sich, welche Maßnahmen von welchem Provider umgesetzt werden müssen.

Interne Zuständigkeiten festlegen

Damit die Provider die TOM im Sinne des Auftraggebers umsetzen und DSGVO-Konformität herstellen, ist ein straffes Providermanagement notwendig. Die Komplexität des Vorhabens hat zur Folge, dass in dessen Phasen (siehe Abbildung 1) verschiedene Expertisen und Rollen benötigt werden, z. B.:

- Geschäftsführung
- Datenschutzbeauftragter
- Vertragsmanagement, Einkauf, Rechtsabteilung
- IT-Sicherheit
- Projektmanager, der die TOM umsetzt
- ITIL-Rollen (Incident Manager, Change Manager, …)
- (operative) Providermanager

Die Regelung von Zuständigkeiten erfolgt idealerweise als Ergänzung einer bestehenden RACI-Matrix.

Providerverträge prüfen

Anhand der definierten TOM (Soll-Zustand) muss dann für jeden einzelnen Providervertrag (Ist-Zustand) mittels Gap-Analyse geprüft werden, ob und welche Vertragsanpassungen jeweils erforderlich sind. Diese müssen generell die DSGVO-Konformität sicherstellen, aber gegebenenfalls auch zusätzliche individuelle Datenschutzrichtlinien des Auftraggebers adressieren. (Im ungünstigsten Fall lassen sich diese nicht durchsetzen – vor allem bei großen Providern außerhalb der EU – sodass ein Providerwechsel oder ein Insourcing erforderlich wird.)

Bei den Vertragsanpassungen müssen der spätere Betrieb und notwendigen Steuerungsinstrumente des Providermanagements bereits berücksichtigt werden.

Maßnahmen umsetzen

Die Umsetzung der Maßnahmen kann Projektcharakter haben und erfordert somit ein professionell arbeitendes (Multi-)Projektmanagement. Es überwacht die Umsetzung von Maßnahmen der einzelnen Provider, leitet Eskalationen bei Abweichungen ein und koordiniert, wenn mehrere Parteien involviert sind.

Providermanagement-Aufgaben im Betrieb

Aus der DSGVO resultieren z. B. die folgenden Aufgaben, für die auf Auftraggeber-Seite die jeweilige Zuständigkeit festgelegt werden muss:

- Verwaltung von Nachweisen, die die in Art. 28 geforderten „hinreichenden Garantien“ belegen (z. B. aktuelles ISO 27001-Zertifikat).
- Kontrollen, dass jeder Provider seinerseits ein Verzeichnis von Verarbeitungstätigkeiten führt (Art. 30).
- Kontrollen, dass jeder Provider festgelegte Verhaltensrichtlinien (Art. 40) umsetzt.
- Providersteuerung und -überwachung bei Prozessen zur Wahrung der Rechte von Betroffenen (Kapitel III, Art. 12 bis 23, Rechte auf Informationen und Auskünfte, Widerspruch, Berichtigung und Löschung von Daten, Einschränkung der Verarbeitung, Datenübertragbarkeit) und bei Beschwerden (Art. 77).
- Mitwirkung bei der Entgegennahme von Informationen vom Provider (Art. 33, Abs. 2) und der Risikobewertung dazu, bei den Meldepflichten gegenüber Aufsichtsbehörden (Art. 33), für die i. d. R. eine Frist von 72 Stunden gilt, und der Information von Betroffenen (Art. 34).
- Bei Schadensersatzforderungen betroffener Personen (Art. 82) kann es um „abschreckende“ Geldbußen gehen (Art. 83). Hierzu müssen vertragliche Regelungen zwischen Auftraggeber und den Providern getroffen werden. Im operativen Betrieb sollte das Providermanagement notwendige Fakten zusammenstellen, um für den Streitfall vorbereitet zu sein.
- Im operativen Betrieb müssen z. B. providerseitige Changes und Sicherheits-Bulletins von Providern auf ihre datenschutzseitigen Auswirkungen hin geprüft werden.

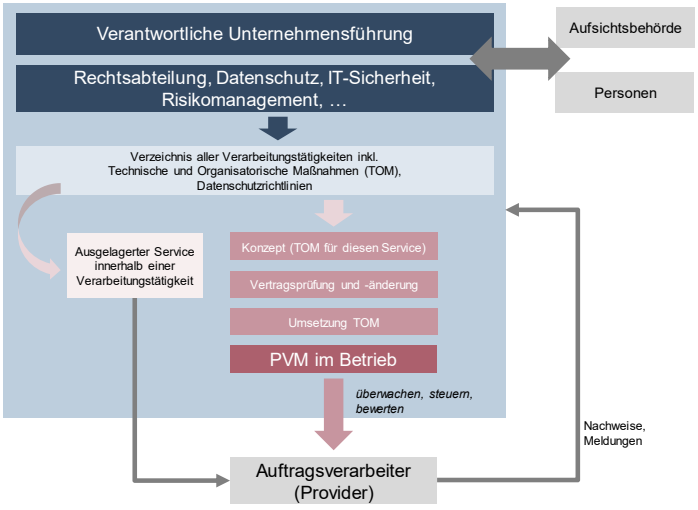


Abbildung 1: Umsetzung der DSGVO beim IT-Outsourcing

Kernaufgabe bleibt die Providerbewertung

Im Kontext der DSGVO sollten neue KPIs aufgenommen und regelmäßig geprüft werden:

- Reaktionszeiten des Providers bei der Umsetzung von TOM
- Zuverlässigkeit bei der Bereitstellung von Garantien gemäß Art. 28 und Zugriff auf das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30
- Reaktionszeiten bei Prozessen zur Wahrung der Rechte von Betroffenen, ggf. aufgeschlüsselt nach Prozess
- Anzahl der Meldungen gemäß Art. 33, Abs. 2 (nach Periode, nach Schweregrad, …)
- Anzahl DSGVO-relevanter Changes auf Providerseite

Fazit

DSGVO in Bezug auf IT-Outsourcing ist ein hochkomplexes Thema, das nicht nur juristische, datenschutzrechtliche und IT-sicherheitstechnische Belange umfasst, sondern auch tiefgehende Kenntnisse im Providermanagement erfordert. Erfolgsfaktoren sind dabei klare Regelungen der Zuständigkeiten, aber auch ein solides ganzheitliches Verständnis: Providermanager müssen die juristische Dimension der DSGVO verstehen. Der Datenschutzbeauftragte wiederum muss wissen, wie Provider bei einem IT-Outsourcing hinsichtlich der Einhaltung des Datenschutzes gesteuert werden.

Michael Schneegans

[1] Bitkom: *Kaum Fortschritt bei der Umsetzung der Datenschutz-Grundverordnung.* [Zugriff am: 21.11.2018]. Verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Kaum-Fortschritt-bei-der-Umsetzung-der-Datenschutz-Grundverordnung.html
[2] DSGVO, Verfügbar unter: https://ec.europa.eu
[3] TeleTrust – Bundesverband IT-Sicherheit e. V.: *IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen.* [Zugriff am: 19.11.2018]. Verfügbar unter: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Unsere Dienstleistungen

amendos Beratung: IT-Compliance-Management

Die Handhabung und Sicherstellung von IT-Compliance stellt – insbesondere in Outsourcing-Situationen – neue Herausforderungen an die interne Organisation: Es ist ein Compliance Management System zu etablieren, das auch die externe Service-Erbringung einbezieht.

Im Rahmen unseres Beratungsangebotes im Bereich IT-Compliance-Management erstellen wir gemeinsam mit Ihnen die hierfür notwendige Konzeption und begleiten deren Umsetzung:

Konzeption eines Compliance-Management-Systems:

- Awareness und Commitment-Workshops für das IT-Management
- Konzeption von Compliance-Richtlinien, Festlegung von Zielen, Maßnahmen zur Verpflichtung aller Beteiligten auf die Ziele
- Hilfe bei dem Aufbau eines internen Compliance-Teams
- Identifikation von relevanten Rechtsnormen und Richtlinien, Zuordnung zu betroffenen – intern und extern erbrachten – IT-Services inkl. Risikoanalyse
- Ableitung von Maßnahmen, Zuordnung von Verantwortlichkeiten und Überwachung von deren Umsetzung

Unterstützung bei der Implementierung der Konzeption

- Training und Weiterbildung Ihrer Mitarbeiter
- Projektmanagement für die Umsetzung der Konzeption
- Beratung und Unterstützung zum Continual Service Improvement
- Beratung zur Optimierung eines bereits operativen IT-Compliance-Managements

Wir beraten Sie gerne:
Tel +49 (0) 40 / 248 276-00
Fax +49 (0)40) / 248 276-01
www.amendos.de
info@amendos.de

DSGVO bei der Nutzung von Cloud-Services

Die DSGVO stellt an Unternehmen hinsichtlich des Datenschutzes zahlreiche neue Anforderungen. Dies gilt umso mehr, wenn das betreffende Unternehmen Cloud-Services nutzt. Welche neuen Anforderungen ergeben sich für Auftraggeber und Auftragnehmer? Was ist bei der Vertragsgestaltung mit einem Cloud-Provider zu beachten? Dies und mehr wird im folgenden Artikel betrachtet.

Die DSGVO bringt keine grundlegende Veränderung in der Frage, welche Verarbeitung personenbezogener Daten zulässig oder unzulässig ist. Die Rechtsgrundlage ändert sich zwar, aber die Prinzipien bleiben grundsätzlich die gleichen. Die Bußgeldhöhe für Verstöße gegen die DSGVO steigt allerdings deutlich an: So beträgt die maximale Geldbuße bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; abhängig davon, welcher Wert der höhere ist.

Der eigentliche, durch die DSGVO ausgelöste Paradigmenwechsel im Datenschutzrecht besteht darin, dass das Datenschutzrecht jetzt umfassende Dokumentations-, Organisations- und Transparenzpflichten vorsieht. Der Auftraggeber muss seine Verarbeitung von personenbezogenen Daten untersuchen. Diese ist auf Unzulässigkeit hin zu überprüfen und/oder verarbeitungsbedingte Risiken sind zu identifizieren und angemessene Maßnahmen zur Risikoreduzierung zu planen und umzusetzen. Daneben gibt es auch Änderungen für bestehende Alt-Verträge sowie veränderte Haftungsregeln.

Im Folgenden werden die wichtigsten Cloud-spezifischen Neuerungen angesprochen:

Seminar

IT-Providermanagement – live im Betrieb: Vertiefendes Praxisseminar

In diesem Seminar erlernen Sie…

- Methoden und Instrumente, um die Zusammenarbeit mit Ihrem IT-Provider profitabler und reibungsfreier zu gestalten,
- die Möglichkeit, durch „learning by doing“ Ihre Kompetenzen als Providermanager zu erweitern und in Simulationen zu trainieren,
- praxisbezogene, im Seminar erarbeitete Task-Sheets zur anschließenden sofortigen Umsetzung.

Termin: 24.09. - 25.09.2019 in Hamburg

Anmeldung: Tel (040) 248 276 00, info@amendos.de

Alt-Verträge

Nach Erwägungsgrund 171 der DSGVO gilt, dass seit 25.Mai 2018 eine Verarbeitung personenbezogener Daten nur noch dann Datenschutz-konform ist, wenn sie den Anforderungen der DSGVO genügt. Somit müssen auch bereits bestehende Verträge mit Cloud-Providern entsprechend der DSGVO gegebenenfalls neu ausgestaltet oder mit Zusätzen versehen werden. Es ist zu überprüfen, ob die eingesetzten Cloud-Provider ihre Verträge selbstständig an die Erfordernisse anpassen und ihre Kunden darüber informieren. Falls nicht, ist die erforderliche Anpassung einzufordern.

Die insgesamt 173 Erwägungsgründe werden zur Auslegung der 99 DSGVO-Artikel herangezogen.

Vorgabe für die Auftragsverarbeitung

Die Auftragsdatenverarbeitung (BDSG-alt) heißt unter der DSGVO nun Auftragsverarbeitung. Bei der Nutzung von Cloud-Services kommt ihr aus datenschutzrechtlicher Sicht eine zentrale Rolle zu. Die Auftragsverarbeitung wird zum größten Teil in den Artikeln 28 und 29 der DSGVO geregelt.

Jede Vereinbarung zwischen Auftraggeber und Service-Provider über Auftragsverarbeitung muss den neuen Anforderungen der Art. 28 / 29 DSGVO genügen.

Gerade im Cloud-Umfeld stellen sich zwei neue Herausforderungen:

- Die Beauftragung von Subunternehmern durch den Auftragnehmer (zum Beispiel für den Cloud-Provider ein Rechenzentrumsbetreiber – IaaS) wird durch Art. 28 DSGVO an strengere Vorgaben geknüpft. Der Auftragnehmer seinerseits hat jetzt dafür Sorge zu tragen – und haftet auch da-für – dass seine Subunternehmer ebenfalls DSGVO-konform vorgehen (Art. 28, Abs. 4 DSGVO). Hierbei ist zu beachten, dass der Verantwortliche (Auftraggeber) den Einsatz von Subunternehmern genehmigen muss (Art. 28, Abs. 2, DSGVO).
- Der Auftragnehmer wird nach Art. 28, Abs. 3e DSGVO unter anderem stärker in die Pflicht genommen, so dass er „… den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte [Informationspflicht, Berichtigung, Löschung u.a.] der betroffenen Person nachzukommen“.

Diesem Umstand sollte bei der Vertragsgestaltung unbedingt Beachtung geschenkt werden. Dies umzusetzen kann allerdings bei den größtenteils hoch standardisierten Cloud-Service-Verträgen der Provider eine Herausforderung sein.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Pflicht zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen trifft nach Art. 25 DSGVO formal den Auftraggeber. Diese Pflicht, geeignete technische und organisatorische Maßnahmen bei der Datenverarbeitung zu ergreifen, wird allerdings faktisch auf den Cloud-Provider „durchschlagen“, da die Umsetzung nicht durch die Nutzung des Cloud-Services allein sichergestellt werden kann. Im besten Fall ist dies bereits im Vertrag geregelt.

Cloud-Services außerhalb der EU

Die Übermittlung personenbezogener Daten in Länder außerhalb der EU (sog. Drittstaaten) wird durch die DSGVO in Art. 44 ff. geregelt. Unverändert bleibt die Zweistufigkeit der Prüfung der Zulässigkeit einer Verarbeitung in Drittstaaten:

- Ist die Verarbeitung durch den Cloud-Provider zulässig (siehe Auftragsverarbeitung – Art. 28)?
- Darf die Verarbeitung im oder der Zugriff aus dem Drittstaat erfolgen (Art. 44 ff. DSGVO)?

amendos IT-Providermanagement

Viele Unternehmen und öffentliche Einrichtungen vergeben immer mehr IT-Services an mehrere externe Provider. Um eine reibungslose Serviceerbringung in der Betriebsphase zu garantieren ist die Etablierung und organisatorische Einbettung eines IT-Providermanagements unerlässlich.

In unserer 9. Ausgabe von **amendos Spezial** dreht sich daher alles um

„Multi-Providermanagement“:

- Sechs Governance-Säulen für das IT-Providermanagement
- Effizientes Multi-Providermanagement
- Agilität und Multi-Providermanagement

amendos Spezial Outsourcing Teil 1

Outsourcing von Teilen der eigenen IT-Leistungen ist in Unternehmen und öffentlichen Einrichtungen keine Seltenheit mehr und macht mittlerweile einen beträchtlichen Anteil der durchgeführten IT-Projekte aus. Deshalb ist es umso erstaunlicher, dass viele Outsourcing-Vorhaben nicht den geplanten wirtschaftlichen Erfolg erzielen. Die Gründe hierfür sind vielfältig.

In dieser Ausgabe von **amendos Spezial** dreht sich daher alles um

„Outsourcing“:

- Risikoanalyse für IT-Outsourcing-Projekte
- Erstellung von Lastenheften und Einholung von Angeboten
- Vermeidung von Fallstricken in der Transition

Diese Prüfung ist entsprechend für jeden Subunternehmer durchzuführen. Bei Cloud-Services würde das bedeuteten: hat ein Provider kein eigenes Rechenzentrum, dann ist der Rechenzentrumsbetreiber der Subunternehmer.

Lesen Sie hierzu auch:

amendos Spezial „Cloud Services“

Eine erfreuliche Situation ergibt sich durch Erwägungsgrund 171 DSGVO. Dieser sieht vor, dass ältere Beschlüsse der EU-Kommission grundsätzlich auch über den Anwendungsbeginn der DSGVO hinaus wirksam bleiben. Das bedeutet insbesondere, dass EU-US Privacy Shield, EU-Standard-verträge und die bereits erfolgte Anerkennung von Drittstaaten mit angemessenem Datenschutzniveau nicht automatisch entfällt, sondern grundsätzlich gilt.

Ausweitung der Haftung des Cloud-Providers durch die DSGVO

Nach dem alten Bundesdatenschutzgesetz hatte der Auftragsverarbeiter eine komfortable Haftungssituation. Ansprüche waren von Betroffenen gegen den Auftraggeber geltend zu machen. Dies wirkte wie eine Haftungsprivilegierung für die Auftragsverarbeiter.

Die DSGVO kennt eine solche Haftungsprivilegierung nicht mehr. Aus Art. 79 DSGVO ergibt sich, dass der Auftragsverarbeiter direkt verklagt werden kann.

Der Art. 82 Abs. 2 DSGVO geht sogar noch einen Schritt weiter:

> Ist sowohl ein Auftraggeber als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

Der Auftragsverarbeiter haftet also gegenüber der betroffenen Person auch für einen Fehler des Auftraggebers.

Lesen Sie hierzu auch:

DSGVO – Missverständnisse und rechtliche Unsicherheiten

Fazit

Wie man sieht, sind durch die DSGVO viele neue Punkte hinzugekommen, die beim Abschluss eines Vertrags mit einem Cloud-Provider, aber auch bei bestehenden Verträgen beachtet werden müssen. Da es sich jedoch gerade im Bereich Cloud-Services oft um standardisierte Verträge handelt, kann dies durchaus eine Herausforderung darstellen und gegebenenfalls dazu führen, dass Provider ausgetauscht werden müssen. Generell sollte das Thema Datenschutz und DSGVO einen großen Bereich in einer möglichen Checkliste für eine Cloud-Migration einnehmen.

Michael Pfitzmann

Impressum

amendos gmbh I Frankenstraße 3 I 20097 Hamburg
Tel (040) 248 276 00 I Fax (040) 248 276 01 I www.amendos.de info@amendos.de Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917

Erscheinungsweise 2 / jährlich I Bezug: kostenfrei als PDF I Copyright: amendos gmbh
Herausgeber und Inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV: Dipl. Oec. Jörg Bujotzek