5FSOFTWARE

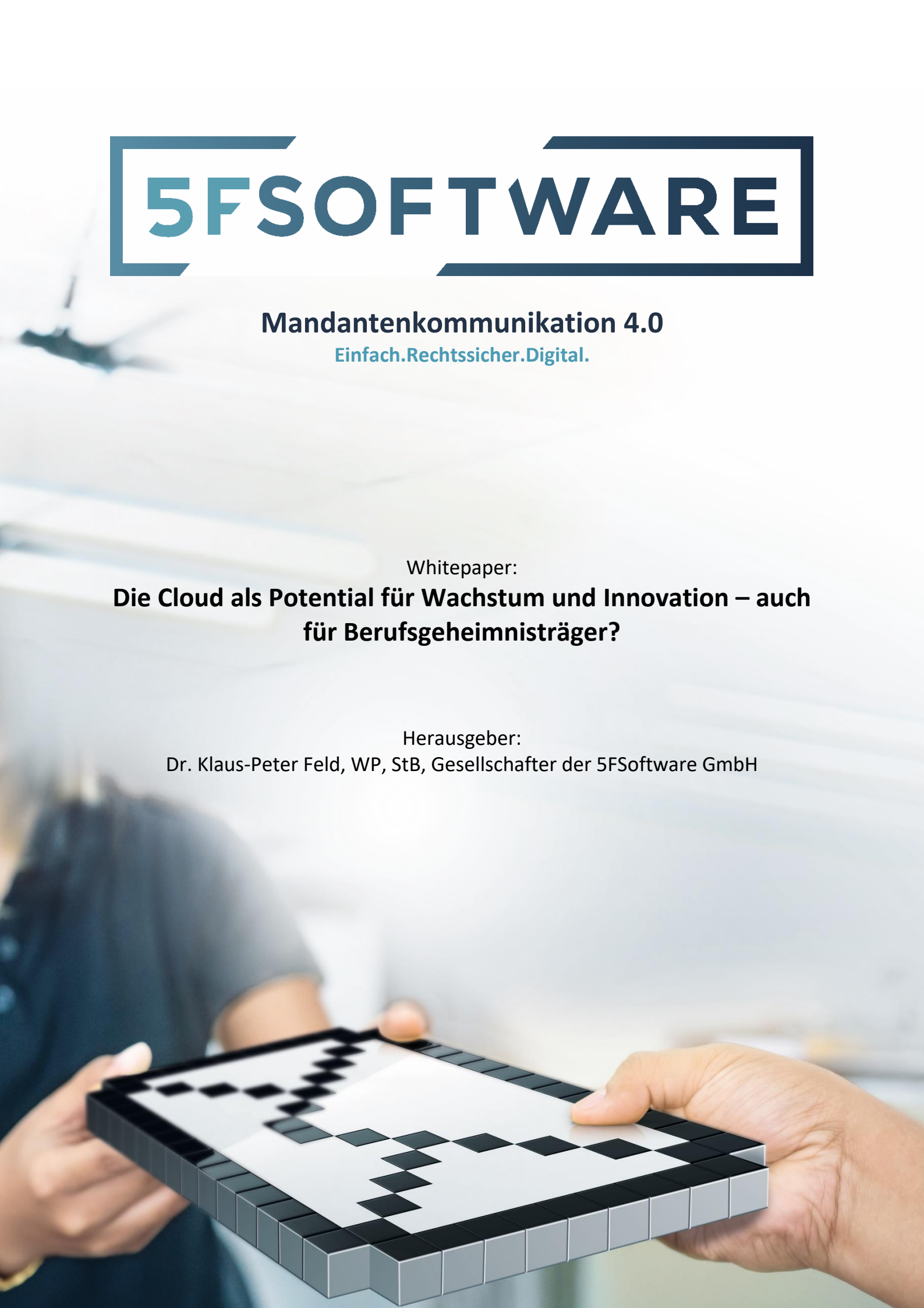
Mandantenkommunikation 4.0

Einfach.Rechtssicher.Digital.

Whitepaper:

Die Cloud als Potential für Wachstum und Innovation – auch für Berufsgeheimnisträger?

Herausgeber:
Dr. Klaus-Peter Feld, WP, StB, Gesellschafter der 5FSoftware GmbH



1. Das Urteil des Markts – Cloud statt on-premise

Schnelles Internet, mobile Endgeräte und die Cloud-Technologie sind der Treibstoff der digitalen Transformation von Wirtschaft und Gesellschaft. Ohne Cloud sowie Mobiles und Internet als ihre „Enabler" ist Digitalisierung „nur" eine Verbesserung, mit Cloud wird sie zur Innovation innerhalb des Unternehmens und über die digitale Vernetzung mit anderen Branchen zu einer Leistung mit Pioniercharakter.

Das Potential der Cloud-Technologie spiegelt sich auch in einem mittlerweile in vollem Gang befindlichen Paradigmenwechsel innerhalb der IKT-Branche wider: Global wurden in 2018 mit Cloud-Services 182 Mrd. US-$ umgesetzt,[1] und allein Amazon Web Services verzeichnete zwischen 2017 und 2018 eine Umsatzsteigerung von rund 17,5 auf 25,7 Mrd. US-$, d.h. um knapp 47%; für Deutschland wird der Umsatz mit Cloud-Computing im B2B-Bereich für das Jahr 2020 mit 22,5 Mrd. € prognostiziert.[2] Laut Cloud Computing Marktbarometer 2019 verlieren demgegenüber „klassische" IT-Lösungen wie Lizenzsoftware, Hardware/Infrastruktur für den On-Premise-Einsatz und IT-Projektgeschäft kontinuierlich an Boden.[3]

Die wachsende Dominanz der Cloud zeigt sich auch darin, dass im Jahre 2018 bereits in nahezu zwei Drittel der deutschen Unternehmen Cloud-Lösungen zum Einsatz kamen und über 70% Public-Cloud-Angebote positiv bewerteten.[4] Insbesondere scheint das Thema „Datenschutz" als in der Vergangenheit oft gehörtes Argument gegen eine (teilweise) Verlagerung der IT in die Cloud an Gewicht zu verlieren, auch wenn trotz eines durch die EU-DSGVO harmonisierten Datenschutzniveaus innerhalb der Europäischen Union ein Rechenzentrumsstandort in Deutschland von Anbieterseite weiterhin als wesentliches Verkaufsargument gesehen wird.[5]

2. Potentiale der Cloud

Welche Gründe stehen hinter dem Trend zur Cloud? Unabhängig davon, ob IT-Anwenderunternehmen eine umfassende Digitalisierungsstrategie verfolgen oder nur begrenzte punktuelle Weiterentwicklungen etablierter Geschäftsmodelle und Prozesse anstreben, ist es in der Regel die betriebswirtschaftliche Überlegenheit gegenüber anderen IT-Bereitstellungsmodellen, die den Ausschlag für die Cloud geben. Entscheidende Bedeutung haben hier vor allem die Schlagworte Skalierbarkeit und Flexibilität. Konkret sind hierfür sich folgende Charakteristika von Cloud-Services ursächlich:

- Allgegenwärtig, bequem und nach Bedarf verfügbar
- Geteilte Ressourcen
- Konfigurierbare Ressourcen
- Schnell produktiv einsetzbar und releasefähig

[1] Vgl. Tenzer, F., Statistiken zum Cloud Computing (https://de.statista.com) , Abruf am 06.07.2019.
[2] Vgl. Tenzer, F., Statistiken zum Cloud Computing (https://de.statista.com) , Abruf am 06.07.2019.
[3] Vgl. Grohmann Business Consulting, Cloud Computing Marktbarometer 2019, S. 8f. (abrufbar unter https://grohmann-business-consulting.de)
[4] Vgl. Tenzer, F., Statistiken zum Cloud Computing (https://de.statista.com) , Abruf am 06.07.2019.
[5] Vgl. Grohmann Business Consulting, Cloud Computing Marktbarometer 2019, S. 14 (abrufbar unter https://grohmann-business-consulting.de)

- Ohne wesentlichen Administrationsaufwand oder Interaktion mit dem Provider nutzbar

Die aus diesen Eigenschaften erwachsenden Potentiale sind erheblich. Zu nennen sind bspw.:

- Schnelle Platzierung neuer digitaler Produkte oder Dienstleistungen am Markt
- Eintritt in neue Märkte ohne erhebliche Investitionen für Infrastruktur und Anwendungen
- In der Folge „low cost to fail" bei Produkteinführungen, Markteintritten oder Einsatz neuer Technologien
- Senkung der IT-Kosten und deren Transformation von Capital Expenditures in Operating Expenditures
- Einfachere fachliche und technische Integration von Partnern
- Zugang zu einem breiten Angebot industriell gefertigter Services und leichte Anpassbarkeit durch Low Code- bzw. No Code-Plattformen
- Kostengünstige Adaption neuer Technologien für eigene und externe Daten (z.B. im Kontext von Data Warehouses, Data Mining, Big Data bzw. Predictive Analytics mittels Machine Learning oder Künstlicher Intelligenz)

3. Cloud als Freund von Compliance, Security und Verfügbarkeit

Nicht zuletzt zu erwähnen ist, dass in der Vergangenheit vielfach – und gerade in Deutschland – die Gewährleistung von Compliance, Security und Verfügbarkeit als Argument gegen die Nutzung von Cloud-Services angeführt wurde. Unbestreitbar ist die mit jedem Auslagerungsmodell verbundene Aufgabe der uneingeschränkten Datenhoheit des Anwenderunternehmens von hoher Sensibilität, und dies bereits ungeachtet gesetzlicher oder regulatorischer Restriktionen, die den Schutz persönlicher Daten oder – im Fall der freien Berufe – die Wahrung von Berufsgeheimnissen gewährleisten sollen.

Auf die Erkenntnis, dass ein höchstmögliches Schutzniveau eine conditio sine qua non für die Marktakzeptanz des Bereitstellungsmodells Cloud darstellt, hat die Anbieterseite indessen in der Breite und konsequent reagiert. Insgesamt kann daher der Befund heute lauten, dass Compliance, Security und Verfügbarkeit in der Cloud sogar besser und kostengünstiger gewährleistet werden können als in traditionellen Rechenzentrums- oder Hostingmodellen. Als State of the Art können insoweit Cloud-Angebote angesehen werden, die folgende Merkmale aufweisen:

- Hochsichere Rechenzentren am Standort Deutschland
- Mehrfache Firewall-Systeme und physische Trennung von Applikations- und Datenservern zum Schutz gegen unberechtigte externe Zugriffe
- Authentifizierung durch Kombination von Benutzernamen und -kennwort sowie ggf. zusätzlich über 2-Faktor-Authentifizierung
- Verschlüsselung der gespeicherten Daten (z.B. nach AES-256)
- Verschlüsselung der Datenkommunikation zwischen Webbrowser des Anwenders und Anwendungsservern des Providers (z.B. SSL/TLS-Verschlüsselung) sowie von Webapplikationen (https) und ggf. Härtung weiterer Kommunikationswege
- Redundanz durch Hot-Stand-By-Serversysteme und räumlich entferntes Ersatzrechenzentrum
- Zugesichertes Datenschutzniveau nach Maßgabe von DSGVO/BDSG
- Regelmäßige Sicherheitsüberprüfungen und Penetrationstests

- Regelmäßige Zertifizierungen durch unabhängige Sachverständige nach anerkannten Sicherheits-Frameworks (z.B. BSI C5, ISO 270X-Familie)

Insbesondere die letztgenannten Zertifizierungen haben eine nicht zu unterschätzende Signalfunktion für die Entwicklung des Cloud-Marktes, da sie einen anders kaum effizient leistbaren Beitrag zum Abbau von Informationsasymmetrien zwischen Anbieter und Nachfrager darstellen. Die Verfügbarkeit aktueller Zertifizierungen ist vor diesem Hintergrund für die Entscheidung von IT Anwenderunternehmen über die Inanspruchnahme von Cloud-Angeboten von zentraler Bedeutung.

4. Berufsgeheimnisträger – kein Sonderfall

Das letztgenannte gilt auch mit besonderem Blick auf die die sogenannten Berufsgeheimnisträger wie Wirtschaftsprüfer, Steuerberater oder Rechtsanwälte als potentielle Nachfrager von Cloud-Angeboten. Nach Auffassung des IDW werden mit den erwähnten Zertifizierungen auch die spezifischen Anforderungen abgedeckt, die sich aus den straf- und berufsrechtlichen Vorgaben bezüglich der Einhaltung der Verschwiegenheitspflicht bei Einschaltung externer Dienstleister ableiten (§ 203 StGB sowie §§ 50a WPO, 62a StBerG, 43e BRAO). Wörtlich wird ausgeführt: „Mithin wird die WP/vBP-Praxis bei (regelmäßigem) Vorlegen aktueller Zertifizierungsnachweise durch das Dienstleistungsunternehmen von der Art und dem Umfang nach angemessenen technischen und organisatorischen Maßnahmen ausgehen können.“[6] Derartige Zertifizierungen erfüllen insoweit vor allem auch die Funktion, dem Berufsgeheimnisträger die ihm vom Straf- und Berufsrecht abverlangte „sorgfältige Auswahl“ des Cloud-Anbieters nachweisen zu können.

Ansonsten gilt generell, dass den Berufsgeheimnisträgern mit der gesetzlichen Novellierung im Jahre 2017 der Weg in die Cloud geebnet werden sollte – ein Weg, der bis dahin hinsichtlich des „ob“ und „wie“ mit rechtlichen Unsicherheiten behaftet war. Tenor der heutigen Regelung ist, die Inanspruchnahme von Cloud-Angeboten nicht an der Verschwiegenheitspflicht scheitern zu lassen, sondern stattdessen mittels vertraglicher „Weiterleitung“, den Provider in ihren Anwendungsbereich einzubeziehen. Für den in der Praxis dominierenden Fall einer durch den Provider nicht höchstpersönlich zu erbringenden Leistung gilt nichts anderes: Mitarbeiter oder Sub-Dienstleister des Providers sind dann lediglich in einer „Weiterleitungskaskade“ ebenfalls zur Verschwiegenheit zu verpflichten.

Auch aus dem gesetzlich verankerten Erforderlichkeitskriterium bzw. „need to know“-Prinzip (Zugang des Dienstleisters zu der Verschwiegenheit unterliegenden Informationen nur, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist) erwachsen keine praktisch relevanten Hürden für die Inanspruchnahme von Cloud-Services. Insbesondere zwingt das Tatbestandsmerkmal der Erforderlichkeit den Berufsgeheimnisträger in keiner Weise, von betriebswirtschaftlich sinnvollen Cloud-Services Abstand zu nehmen. Lediglich soll verhindert werden, dass dem Provider mehr als das für die Leistungserbringung Notwendige offenbart wird.

An dieser Stelle erscheint zudem die Klarstellung angebracht, dass ein „Offenbaren“ ohnehin nur dann vorliegt, wenn hierdurch die inhaltliche Kenntnisnahme des der Verschwiegenheit unterliegenden Lebenssachverhalts vermittelt oder zumindest ermöglicht wird. Hieran fehlt es indessen, wenn – wie typisch für viele Cloud-Services – Daten ausschließlich in

[6] Vgl. IDW, Hilfestellung zur Beauftragung von Dienstleistern, S. 31 (abrufbar unter http://idw.de).

verschlüsselter, fragmentierter, anonymisierter, pseudonymisierter oder in anderer Weise, die die Kenntnis von ihrem tatsächlichen Inhalt ausschließt, übertragen, verarbeitet und gespeichert werden. Hat in solchen Fällen der Provider auch keine Möglichkeit der bedarfsweisen Kenntlichmachung (z.B. mittels Entschlüsselung), sind § 203 StGB und seine berufsrechtlichen Pendants von vorneherein und insgesamt nicht einschlägig. Anderenfalls liegt die Lösung in einer (praxisüblichen) Beschränkung des Gebrauchs der Möglichkeiten zur Kenntlichmachung, die mit dem „need-to-know"-Prinzip im konkreten Einzelfall vereinbar ist (z.B. Beschränkung auf Notsituationen oder für Wartungszwecke).

5. Fragen für potentielle Cloud-Nutzer im Überblick

Als Handlungsempfehlung kann festgehalten werden: Bei der Entscheidung über die Substitution traditioneller Bereitstellungsmodelle durch Cloud-Lösungen sollten sich IT-Anwenderunternehmen insbesondere über folgende Fragestellungen Klarheit verschaffen: [7]

- Welche **Funktionen** sind künftig durch den Cloud-Provider zu erbringen und werden darüber hinaus **Funktionsausweitungen** angestrebt?
- Wie werden die **Verfügbarkeit** übertragener Funktionen und die **Anforderungen an einen ordnungsgemäßen der IT-Betrieb** (Integrität, Authentizität und Verbindlichkeit) gewährleistet?
- Welche **ökonomischen Ziele** (z.B. Kostensenkungen) sollen mit der Cloud-Lösung erreicht werden?
- Inwieweit entfällt durch die Cloud-Lösung die Notwendigkeit zum Aufbau bzw. Aufrechterhaltung von **technischem Spezialknowhow** außerhalb der Kernkompetenzen des IT-Anwenderunternehmens?
- Inwieweit macht die Skalierbarkeit der Cloud-Lösung die interne Bereitstellung **personeller und technischer Ressourcen** (z.B. IT-Fachkräfte, Speicherkapazität, Rechnerleistung) verzichtbar?
- Welchen Beitrag leistet die Cloud-Lösung zur Realisierung **technischer Innovationen**?
- Welchen Beitrag leistet die Cloud-Lösung zur Abwehr gestiegener IT-Sicherheitsrisiken (z.B. infolge der gestiegenen Bedrohungen durch Cybercrime)?
  - Wie werden **Geschäftsgeheimnisse oder andere wettbewerbsrelevante Informationen** vor unberechtigtem Zugriff Dritter geschützt?
  - Wie wird die Einhaltung **datenschutzrechtlicher Vorgaben** gewährleistet?
  - Wie wird – sofern für das IT-Anwenderunternehmen einschlägig – der straf- und berufsrechtliche **Berufsgeheimnisschutz** gewährleistet

[7] Vgl. IDW, Hilfestellung zur Beauftragung von Dienstleistern, S. 32 ff. (abrufbar unter http://idw.de).

Mandantenkommunikation in der Cloud?

Sie wollen Ihre Mandantenkommunikation digitalisieren? Mit 5FSoftware haben Sie einen Partner an Ihrer Seite, der Ihnen hilft Abläufe in der Mandantenkommunikation einfacher und effektiver zu gestalten. Egal ob einfaches Teilen eines Dokumentes, zur Ansicht zur Verfügung stellen oder das Einsammeln von Dokumenten beim Mandanten über konfigurierbare Checklisten.

Wir legen höchsten Wert auf die Datensicherheit und den deutschen Datenschutz.
Von Berufsträgern für Berufsträger.

Vereinbaren Sie eine kostenlose unverbindliche Einführung und lernen Sie die 5F Lösung zur Mandantenkommunikation kennen.

Gleich unter www.5fsoftware.de/beratung/ einen Termin anfordern und profitieren.

Wir freuen uns auf Sie!

5FSOFTWARE