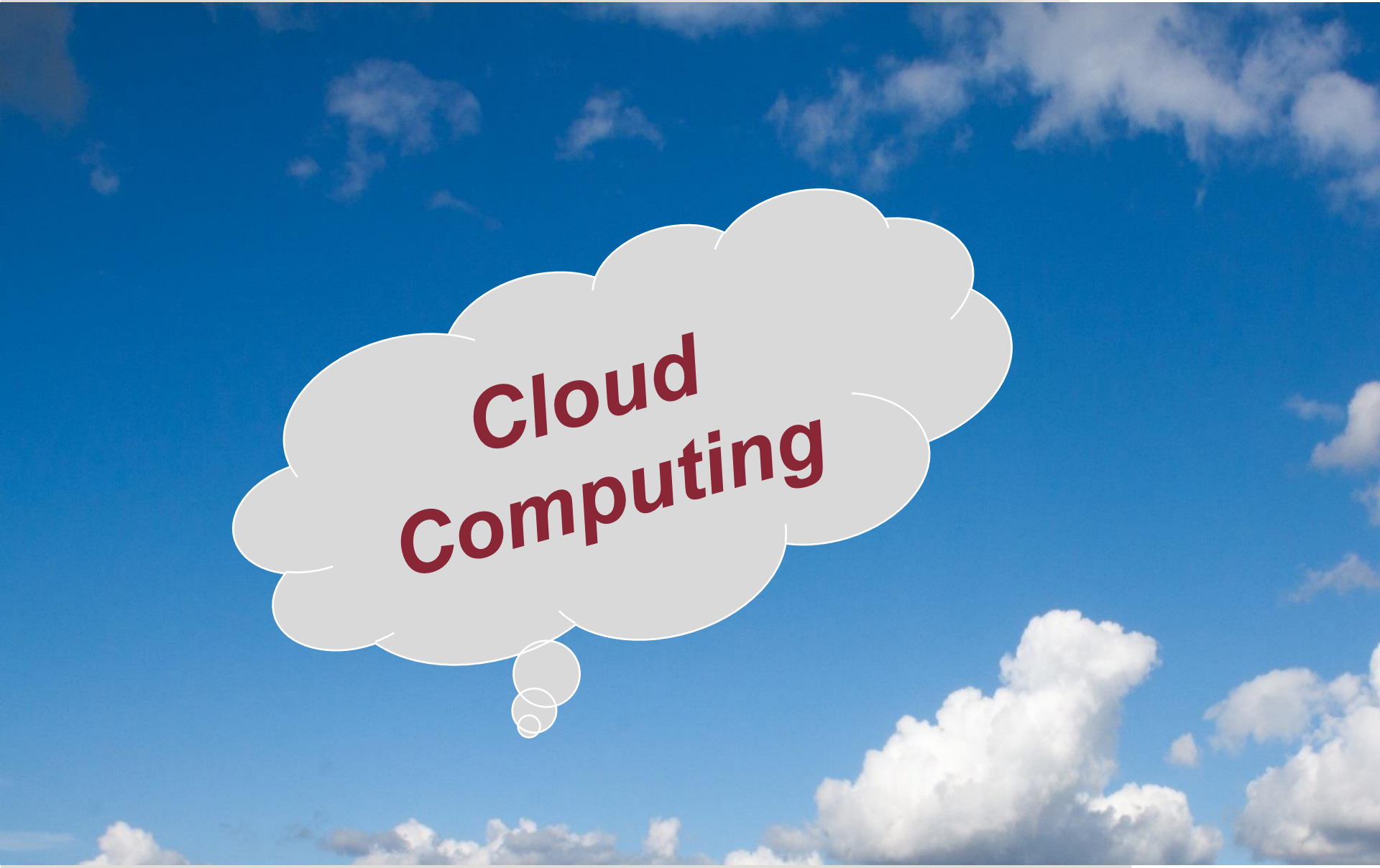
Cloud Computing in der ERGO

Vortrag im Rahmen Forum V
Juristisches Kolloquium an der Friedrich-Alexander-Universität
Nürnberg, 14. Februar 2019

Thomas Schick
ERGO Group AG / Group Legal
Leiter Vertriebsrecht, Datenschutz, Digital Ventures

ERGO


Cloud
Computing

Definition Cloud / Cloud Computing

ERGO

Der Begriff „Cloud“ umschreibt:

- **ein globales Netzwerk von Servern, die alle eine eigene Funktion erfüllen**
- **die Server sind dazu ausgelegt, Daten zu speichern oder zu verwalten**
- **die Cloud kann von jedem internetfähigen Gerät online erreicht werden**

Bekannte Cloudanbieter sind z.B. Amazon Web Service (AWS), Salesforce, Microsoft, IBM, SAP, Telekom. Diese Cloudanbieter bieten die Möglichkeit, dass entweder eine Privatperson oder ein Unternehmen Daten in deren Rechenzentren gegen Gebühr speichern kann.

Cloud Computing ist ein sich entwickelnder Begriff, der die Entwicklung vieler vorhandener Technologien und Ansätze für das Computing zu etwas Neuem beschreibt.

Einkauf von externen Speicherkapazitäten und Technologien

Warum Cloud Computing und nicht alles on premise?

ERGO

Für Versicherungsunternehmen ist Cloud Computing interessant, da

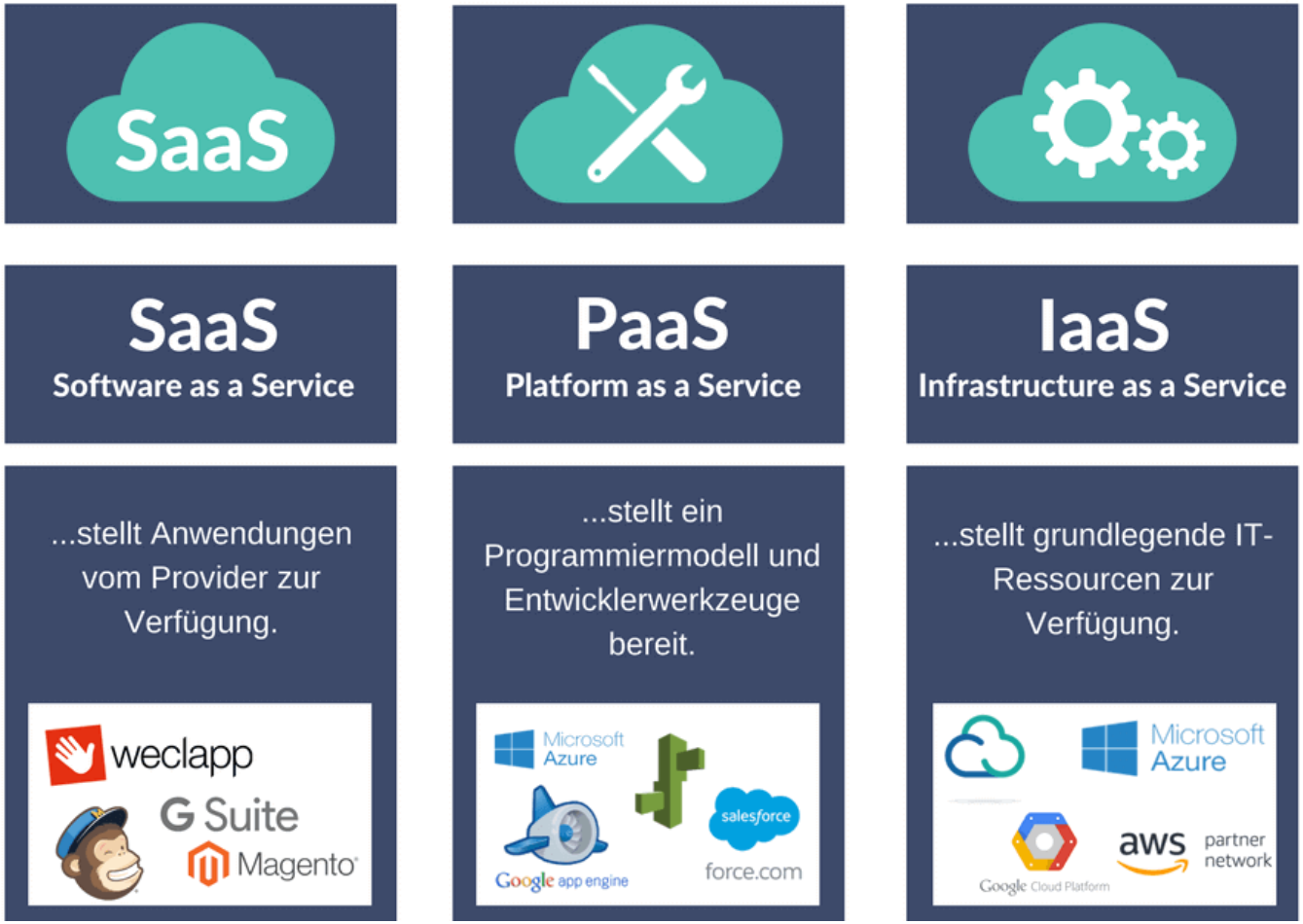
- **es die Alternative eröffnet, Daten außerhalb der eigenen Rechenzentren zu speichern oder zu verwalten und**
- **die Möglichkeit besteht, Kosten zu reduzieren und moderne Technologien nutzen zu können (gutes Kosten/Nutzenverhältnis).**

Bereitstellen, Wartung und Support von Rechenleistung werden ausgelagert. Technische Neuerungen können schneller und zu günstigeren Kosten realisiert werden.

Cloud Computing ist ein wichtiger Baustein bei der voranschreitenden Digitalisierung im Versicherungsmarkt. Digitalisierung benötigt Rechenleistung.

Kostenreduzierung und schnelle Nutzung moderner Technologien

Welche Cloud Computing Typen gibt es?



Quelle: 2018 weclapp

Welche Cloud Computing Typen gibt es?

Infrastructure as a Service (IaaS)

- **Basis** für alle Cloud-Service-Modelle
- **virtuelle Infrastruktur-Komponenten** (**Rechen- und Speicherleistung)** finden auf virtualisierten Servern statt und der Umfang kann vom nutzenden Unternehmen jederzeit an den Bedarf angepasst werden.
- **Kontrolle**: volle Kontrolle über das IT-System vom Betriebssystem aufwärts beim Anwender; „nur“ Kontrolle über physikalische Umgebung liegt beim Cloud-Anbieter

Plattform as a Service (PaaS)

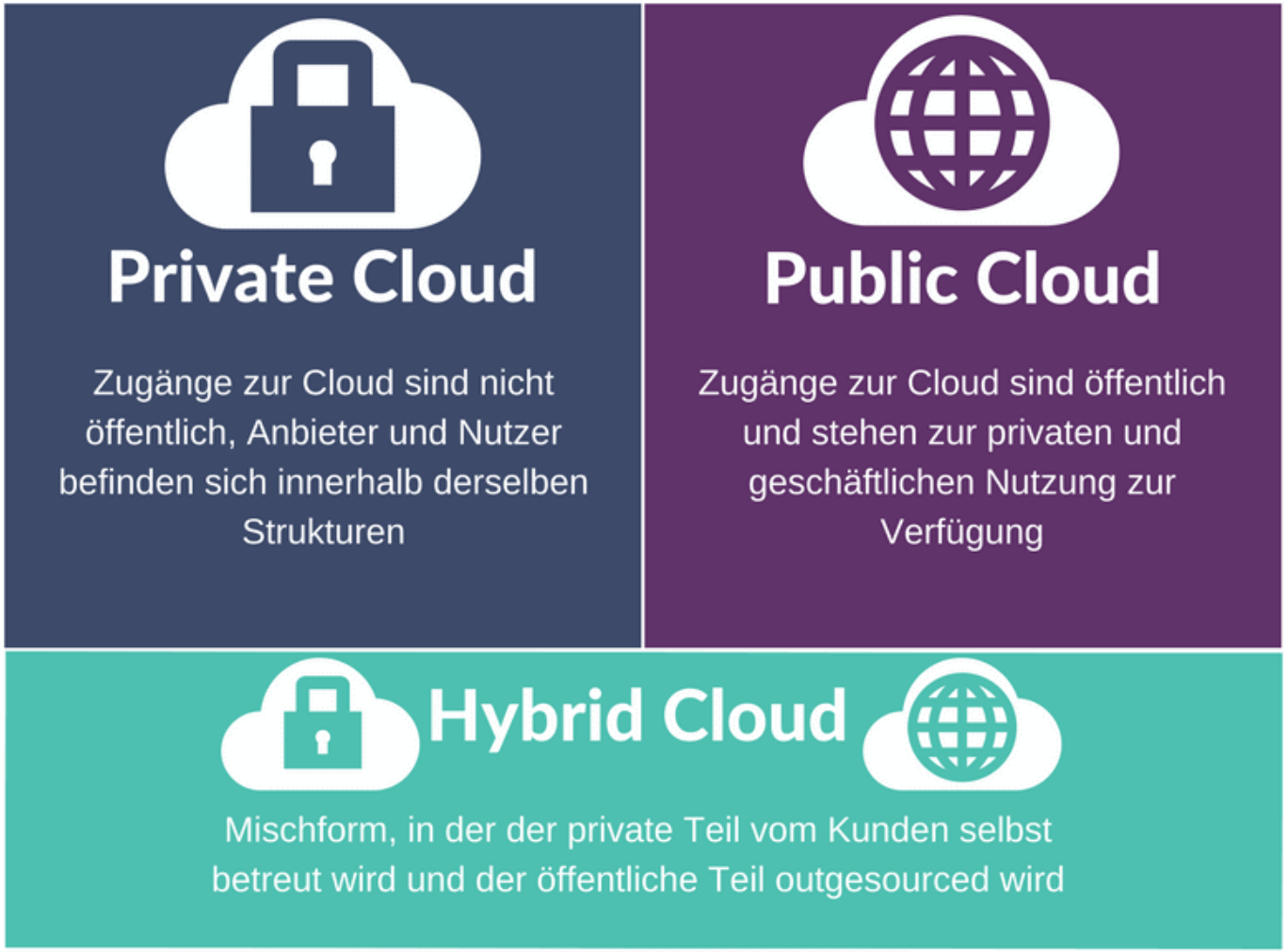
- Zugriff auf eine Entwicklungsumgebung, in dem der Anwender **eigene Applikationen entwickeln** und betreiben kann.
- Entwicklungsprozess selbst und die Programmierung findet allerdings außerhalb des Unternehmens statt.
- Anwendungen werden auf den Servern des Unternehmens betrieben.
- **Kontrolle**: Anwender hat (nur) Kontrolle über seine Anwendungen; Kontrolle über Betriebssystem liegt beim Cloud-Anbieter

Software as a Service (SaaS)

- **Auslagerung** einer **einzelnen Anwendung** bis hin zur **Auslagerung der kompletten Unternehmens-IT**
- Auch Anwendungen und Daten sind in der Cloud und somit auf den Servern des Cloud-Anbieters.
- Anwender mietet die Software aus dem Internet nach Bedarf als **„Software on Demand“**
- Angebot an SaaS-Lösungen aus der Cloud reicht von Office- und Kollaborationslösungen bis hin zu Unternehmenssoftware (ERP-Systeme)
- **Kontrolle**: „praktisch“ übergibt der Anwender die vollständige Kontrolle an den Cloud-Anbieter

BaFin: „*Ein Verlust von Kontrolle ist nicht gleichzusetzen mit einem Verlust von Verantwortlichkeit im aufsichtsrechtlichen Sinne.“*

Welche Cloud Computing Modelle gibt es?



Quelle: 2018 weclapp

Rechtliche Herausforderungen beim Cloud Computing

Die Einschaltung von (externen) Dienstleistern unterliegt diversen regulatorischen und rechtlichen Anforderungen. Zu berücksichtigen sind insbesondere:

Datenschutz (EU-DSGVO / BDSG neu)
- Vereinbarung zur Auftragsverarbeitung
- technische und organisatorische Maßnahmen (TOMs) zur Sicherheit

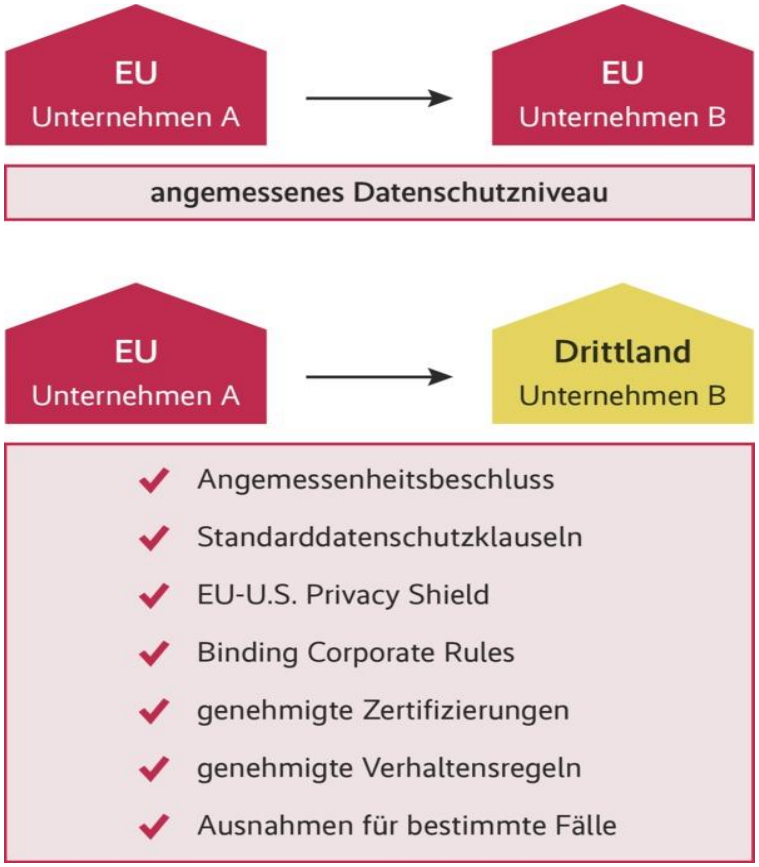
Strafrecht
Schweigepflicht (§ 203 StGB)
Verpflichtung von Dienstleistern zur Geheimhaltung

Aufsichtsrecht (VAG)
Aktuell: Orientierungshilfe der BaFin zum Cloud Computing

1. Datenschutzrecht

Bei (IT-)Dienstleistungen ist immer zu prüfen, ob personenbezogene (pb) Daten verarbeitet werden.

- **Wenn ja – Erstellen einer Beschreibung der Verarbeitungstätigkeit.**
  - ➡ **Konkrete Angaben welche Daten, wie und wo durch den Dienstleister (DL) im Auftrag der ERGO verarbeitet werden**
- **Dienstleister aus der EU:**
  - ➡ **Abschluss einer Vereinbarung zur Auftragsverarbeitung (VAV) ausreichend**
- **Dienstleister aus „Non EU“:**
  - ➡ **Das Datenschutzniveau der EU muss erreicht werden (Art. 44 ff DSGVO)**



2. Strafrecht

Ende 2017 wurde § 203 StGB reformiert

- **Berufsgeheimnisträgern – wie z.B. private Kranken-, Leben- oder Unfallversicherer – ist erlaubt, neben den berufsmäßig tätigen Gehilfen auch „sonstige Personen“ (also auch Dienstleister) einzuschalten**

- **Diese Dienstleister und ihre Subunternehmer müssen zur Geheimhaltung verpflichtet werden**

- **Auswirkungen auf Versicherungsunternehmen wie ERGO, die von § 203 StGB erfasst werden (z.B. ERGO Versicherung AG, DKV, ERGO Vorsorge, ERGO Direkt Krankenversicherung AG), auf die konzerneigenen Dienstleister dieser Versicherer (z.B. ERGO Group AG als Holdinggesellschaft, konzerneigene IT-Dienstleister) und die externen Dienstleister**

Rechtliche Herausforderungen beim Cloud Computing

ERGO-Mustertext zur Verpflichtung nach § 203 StGB

Einbindung in (neue) **Vereinbarungen zur Auftragsverarbeitungen (VAV)** bzw. getrennte / nachträgliche Vereinbarung:

„Der Verantwortliche hat den Auftragsverarbeiter darüber informiert, dass der Verantwortliche als zentraler Dienstleister der ERGO Group auch Aufgaben für private Kranken-, Leben- bzw. Unfallversicherer übernimmt. Die Angehörigen dieser privaten Versicherer unterliegen einer strafbewährten Schweigepflicht nach § 203 Absatz 1 Nr. 7 StGB. Nach dieser Vorschrift macht sich ein Angehöriger strafbar, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm in dieser Funktion anvertraut worden oder sonst bekanntgeworden ist. Zu den geheimhaltungsbedürftigen Informationen zählen sowohl die zum persönlichen Lebensbereich der einzelnen Versicherten gehörenden Geheimnisse als auch Betriebs- oder Geschäftsgeheimnisse. Bereits die Tatsache, dass eine Person bei einem Versicherer eine entsprechende Kranken-, Leben- bzw. Unfallversicherung unterhält, ist ein solches Geheimnis. Daneben sind grundsätzlich sämtliche Informationen geheimhaltungsbedürftig, die im Laufe eines solchen Versicherungsverhältnisses anfallen – z.B. sämtliche Angaben über Vertragsinhalte, Leistungsfälle oder Unfallmeldungen. Das Verwerten eines solchen Geheimnisses ist nach § 204 StGB strafbar.

Darüber hinaus hat der Verantwortliche den Auftragsverarbeiter belehrt, dass neben den Angehörigen des jeweiligen Versicherers auch sonstige Personen, die an der beruflichen Tätigkeit des Versicherers mitwirken, der strafbewährten Schweigepflicht nach § 203 Absatz 4 Satz 1 StGB unterliegen. Diese Schweigepflicht gilt somit sowohl für den Verantwortlichen als zentralen Dienstleister als auch für den Auftragsverarbeiter als Subunternehmer.

Der Auftragsverarbeiter verpflichtet sich, die dargelegte Schweigepflicht (vgl. §§ 203, 204 StGB) zu beachten und alle geheimhaltungsbedürftigen Informationen streng vertraulich zu behandeln. Daneben wird der Auftragsverarbeiter seine Mitarbeiter zur Verschwiegenheit verpflichten und diese auf die strafrechtlichen Folgen eines Verstoßes hinweisen.

Der Auftragsverarbeiter wird sich nur insoweit Kenntnis von entsprechenden Geheimnissen verschaffen, als dies zur Erfüllung der von ihm übernommenen vertraglichen Aufgaben erforderlich ist.

Sofern der Auftragsverarbeiter weitere Subunternehmer zur Erfüllung der von ihm vertraglich übernommenen Aufgaben heranzieht, wird er diese ebenfalls zur Verschwiegenheit verpflichten und auf die strafrechtlichen Folgen eines Verstoßes hinweisen. Der Auftragsverarbeiter wird mit dem Subunternehmer vertraglich vereinbaren, dass dieser seine Mitarbeiter zur Verschwiegenheit verpflichtet und auf die strafrechtlichen Folgen eines Verstoßes hinweist. Die vertraglichen Regelungen zur Einschaltung von Subauftragsverarbeitern nach § 5 der VAV bleiben hiervon unberührt."

Rechtliche Herausforderungen beim Cloud Computing

3. Aufsichtsrecht

- **Eine Auslagerung (Ausgliederung, § 32 VAG) darf nach den aufsichtsrechtlichen Anforderungen nicht zu einer Übertragung der Verantwortung der Geschäftsleiter des beaufsichtigten Unternehmens für die ausgelagerten Sachverhalte an den Cloud-Anbieter führen.**
- **Das beaufsichtigte Unternehmen bleibt bei einer Auslagerung für die Einhaltung der vom beaufsichtigten Unternehmen zu beachtenden gesetzlichen Bestimmungen weiterhin verantwortlich.**

  Insofern muss das Versicherungsunternehmen gegenüber dem Cloudanbieter insbesondere folgendes sicherstellen*:
  - **Weisungsrecht bzgl. seiner Daten**
  - **Uneingeschränktes Informations- und Auskunftsrecht im Hinblick auf die ausgegliederten Tätigkeiten**
  - **Weitergehende Eingriffsrechte für die Aufsichtsbehörde BaFin und das Versicherungsunternehmen: Kontrollrechte für interne und externe Prüfer, Zutrittsrechte**
  - **die Aufsichtsbehörde kann Kündigung gegen den Willen des Dienstleisters erzwingen**

* **BaFin Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter**
(https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.html)

3. Aufsichtsrecht

I. Risikoanalyse und Wesentlichkeitsbewertung der Ausgliederung

Kriterien* sind u.a.:

- ✓ **Kritikalität, d.h. ist der Sachverhalt für die Geschäftsfortführung kritisch?**
- ✓ **Risikobewertung aus dem gewählten Modell (z.B. IaaS, PaaS, SaaS / Public oder Private Cloud)**
- ✓ **Finanzielle, operationelle Risiken (Systemausfall, Sabotage)**
- ✓ **Rechtliche Risiken (Datenschutz, Rechtsdurchsetzung), Reputationsrisiken**
- ✓ **Bewertung/Eignung des Cloud-Dienstleisters (wirtschaftliche Situation, regulatorischer Status, Infrastruktur), Zertifikate, Prüfberichte Dritter, Kumulrisiken, etc.**
- ✓ **Geopolitische Lage (Stabilität des Landes)**
- ✓ **Integrität, Verfügbarkeit, Vertraulichkeit des Anbieters, etc.; z.B. Risiken aus Schnittstellen zw. den Systemen, Datenverlust oder eingeschränkte (Rück)Übertragbarkeit der Daten**
- ✓ **…**

* BaFin Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

ERGO

3. Aufsichtsrecht

II. Vertragsgestaltung*

1. Leistungsgegenstand und SLA

- ✓ Beschreibung des auszulagernden Sachverhalts
- ✓ Ort der Leistungserbringung
- ✓ Indikatoren zum Leistungsniveau, um mangelhafte Leistungen zu erkennen

2. Informations- und Prüfungsrechte

- ✓ Sicherstellen, dass alle erforderlichen Informationen zur Überwachung und Steuerung gegeben werden
- ✓ Uneingeschränkter Zugriff auf alle Informationen und Daten sowie Zugang zu den Räumen des Anbieters
- ✓ Durchführung von Vor-Ort-Prüfungen
- ✓ Keine (mittelbare) vertragliche Einschränkung der Prüfrechte
- ✓ Erleichterungen durch Pooled Audits, Nachweise/Zertifikate, Prüfberichte, etc. möglich; aber nicht ausschließlich

3. Informations- und Prüfrechte der Aufsicht

- ✓ Aufsicht muss den Anbieter genauso kontrollieren können wie das beaufsichtigte Unternehmen
- ✓ Uneingeschränkte Zusammenarbeit mit der Aufsicht
- ✓ Uneingeschränkter Zugang zu Informationen, Daten und Geschäftsräumen
- ✓ Keine (mittelbare) vertragliche Einschränkung der Prüfrechte

4. Weisungsrechte

- ✓ Daten dürfen nur im Rahmen der Weisungen verarbeitet werden
- ✓ Berichtigung, Löschen und Sperren von Daten
- ✓ Einfluss auf Umfang von Zertifizierungen oder Prüfberichten

* BaFin Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

Rechtliche Herausforderungen beim Cloud Computing

ERGO

3. Aufsichtsrecht

5. Datensicherheit/Datenschutz

- ✓ Ort der Datenspeicherung, konkreter Standort des Rechenzentrums (Stadt)
- ✓ Sicherstellen der Redundanz der Daten und Systeme für den Fall eines Ausfalls
- ✓ Jederzeitiger Zugriff auf die Daten und Möglichkeit der Rücküberführung, Kompatibilität der Systeme

6. Kündigung

- ✓ Angemessene ordentliche Kündigungsfristen
- ✓ Kündigungsrecht aus wichtigen Grund, wenn die Aufsicht die Beendigung verlangt
- ✓ Löschen der Daten nach Rückübertragung

7. Weiterverlagerung

- ✓ Zustimmungsvorbehalt einräumen
- ✓ Nur möglich, wenn Informations- und Kontrollrechte auch uneingeschränkt beim Subdienstleister gelten
- ✓ Überprüfung der Risikoanalyse (Erhöhung des Risikos durch Subdienstleistung?)

8. Informationspflichten

- ✓ Z.B. Meldung von Störungen oder Gefahren für die Sicherheit der Daten
- ✓ Angemessene Vorabinformation bei relevanten geplanten Änderungen durch den Cloud-Anbieter

9. Anwendbares Recht

- ✓ Deutsches Recht oder zumindest Recht eines Staats in der EU/EWR

* BaFin Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

Cloud Computing in ERGO

- **ERGO hat die regulatorischen und rechtlichen Anforderungen in einer eigenen, internen „Cloud-Richtlinie“ zusammengestellt. Diese ist vom Vorstand der ERGO Group AG verabschiedet. Die festgelegten Bedingungen („Cloud-Prinzipien“) sind bei allen Cloud-Nutzungen einzuhalten.**

- **ERGO hat 2016 einen sog. Cloud Governance Prozess (CGP) entwickelt, um die Prüfung und Einhaltung der regulatorischen und rechtlichen Anforderungen / internen “Cloud-Richtlinie” sicherzustellen.**

Cloud Principles und Cloud Governance Prozess

ERGO - Cloud Principles

Cloud Prinzipien

1	Begrenzte Datenverarbeitung – je nach Datenart werden sämtliche regulatorischen / rechtlichen Anforderungen sowie interne Vorgaben zur Informationsklassifizierung beachtet
2	Dienstleister / Rechenzentren (RZ) sind rechtlich geprüft
3	Standardmäßige Verschlüsselung – risikobasierter Ansatz
4	Angemessene Zertifizierungen und Prüfungsrechte
5	Portabilität und Verfügbarkeit von Cloud-Lösungen
6	Starke Cloud-Governance – ggf. Risikoübernahme durch Vorstand möglich

ERGO - Cloud Principles - Beispiele

Cloud Prinzipien

- **Begrenzte Datenverarbeitung**

Nur so viele Daten, wie nötig sind, werden extern gespeichert; Informationsklassifizierung bedeutet Kategorisierung von Daten in öffentlich, intern, vertraulich und streng vertraulich

- **Dienstleister / Rechenzentren sind rechtlich geprüft**

Für die RZ des Cloud-Anbieters auf deutschem Boden liegen entsprechende Zertifizierungen vor, wie ISO 27001 usw.

- **Standardmäßige Verschlüsselung – risikobasierter Ansatz**

Je sensibler die Daten sind, desto höher und besser muss der Grad der Verschlüsselung sein.
Streng vertrauliche Daten können von uns mit einem eigenen Verschlüsselungsverfahren als einstellende Stelle in das fremde RZ eingestellt werden

- **Angemessene Zertifizierungen und Prüfungsrechte**

Zu Zertifizierung siehe Punkt 2. Wir stellen sicher, dass wir Informationen vom Cloud-Anbieter erhalten, die wir für die angemessenen Steuerung und Überwachung der Risiken im Sinne des Aufsichtsrechts brauchen

- **Portabilität und Verfügbarkeit von Cloud-Lösungen**

In den Verträgen mit dem Cloud-Anbieter wird geregelt, dass die Daten so schnell es möglich ist, woanders hin (z.B. ins eigene RZ) übertragen werden können. Die Verfügbarkeit des externen RZ sollte 24/7 gewährleistet sein

- **Starke Cloud-Governance – ggf. Risikoübernahme durch Vorstand möglich (Business Judgement Rule)**

Wenn einzelne Prinzipien nicht zu 100 % erfüllt werden können, kann der Vorstand des verantwortlichen ERGO-Unternehmens das Risiko übernehmen

ERGO - Cloud Governance Prozess (CGP)

In den CGP sind sämtliche Einheiten (“Stakeholder”) eingebunden, die regulatorische und rechtliche Anforderungen beurteilen bzw. deren Einhaltung sicherstellen.

Dies sind:

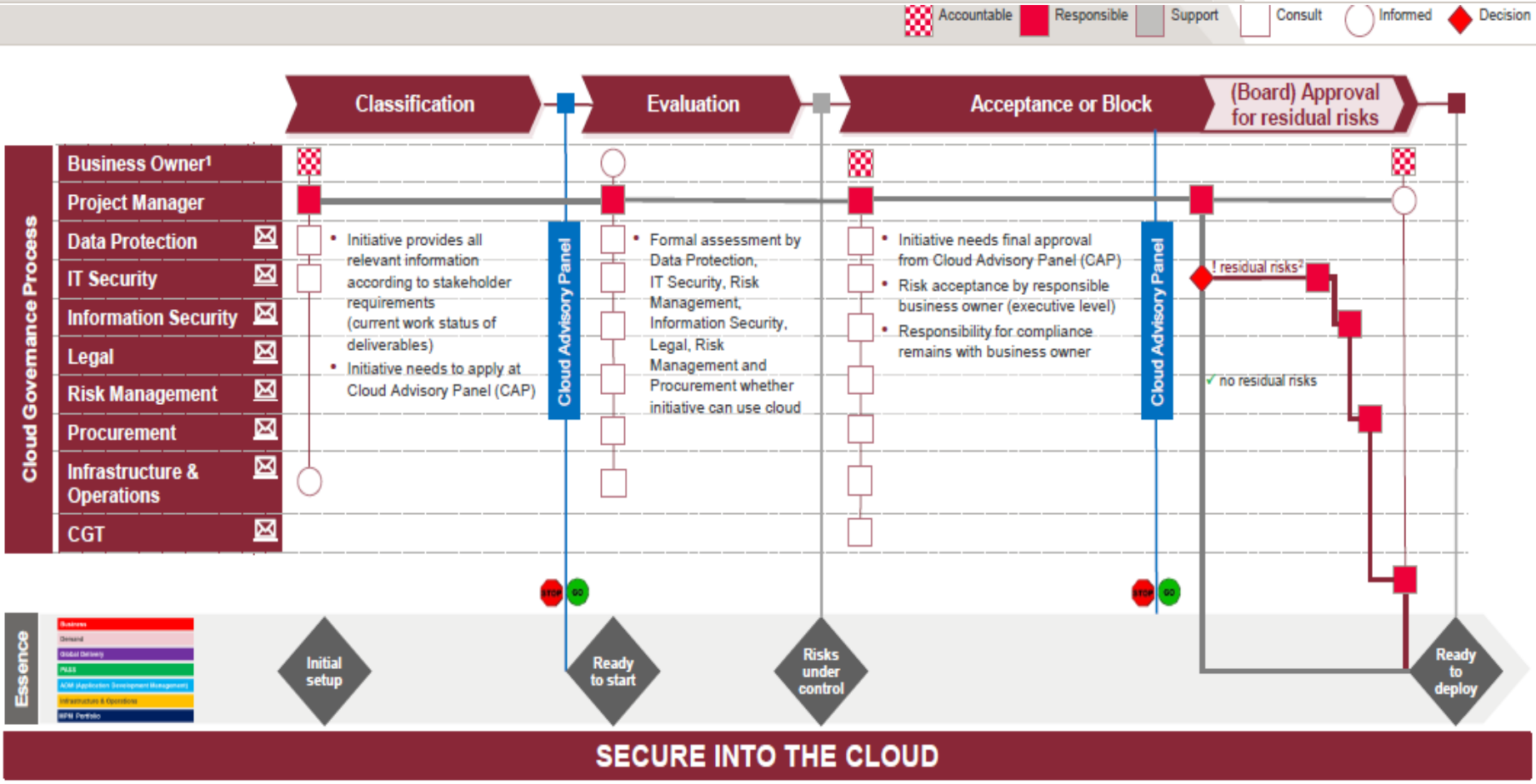
- **Legal / Data Protection**
- **IT-Security / Information Security**
- **Internes Risk Management (IRM)**
- **Procurement**
- **Infrastructure & Operations**

- **Jedes Projekt, das Cloud Computing nutzen möchte, muss den CGP durchlaufen.**
- **Sämtliche Stakeholder treffen sich 14tägig im Cloud Advisory Panel (CAP). Alle Projekte stellen sich im CAP vor.**
- **Ein “go live” findet erst nach einer finalen Freigabe durch das CAP statt.**
- **Bei festgestellten / verbleibenden (Rest-)Risiken kann eine Risikoübernahme – je nach Höhe – durch den Projekt-Owner oder den zuständigen Vorstand erfolgen.**

Der CGP stellt sicher, dass jede Cloud-Initiative durch wichtige Unternehmensbereiche bewertet und freigegeben wird sowie der Business Owner / Vorstand etwaige Restrisiken übernimmt.

Cloud Governance Process (CGP)

Übersicht – Ablauf und Organisation (1)

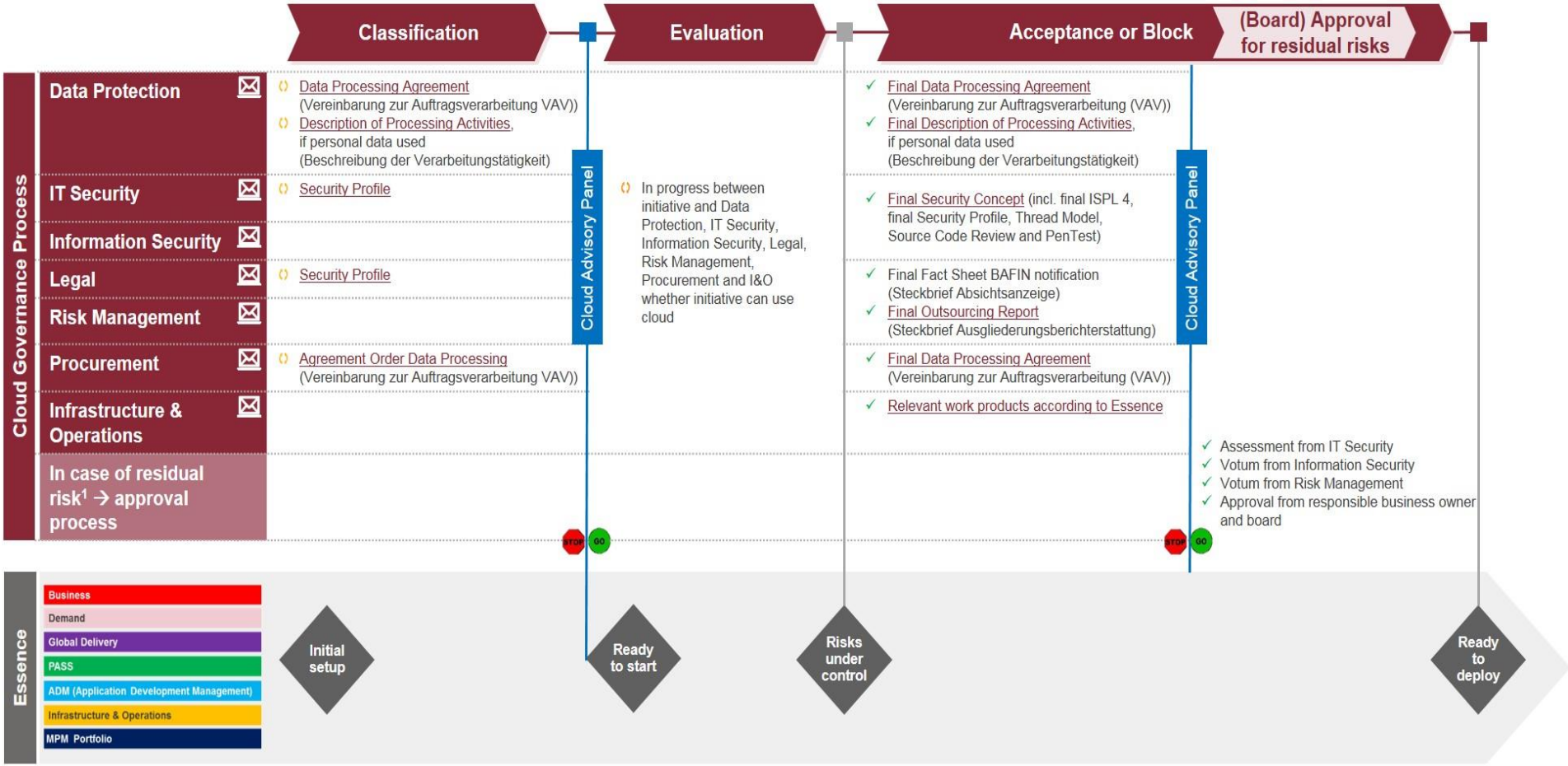


¹ Business Owner: executive responsible for business process

² Residual Risk: deviation from policy ISPL3

Cloud Governance Process (CGP)

Übersicht – Ablauf und Organisation (2)



[1] Residual Risk: deviation from policy ISPL3

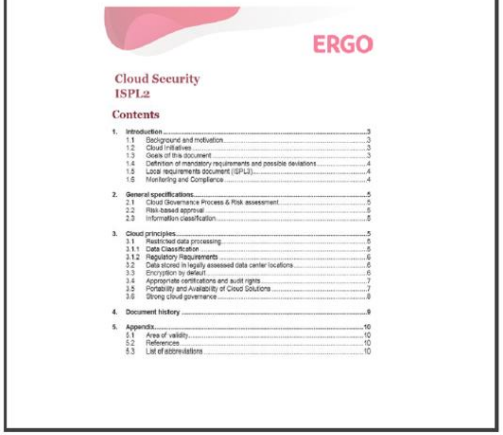
Cloud Governance Process (CGP)

Übersicht – Ablauf und Organisation (3)

ERGO

Cloud Projekte müssen die Anforderungen der Richtlinien „ISPL2-Cloud Security“ und „ISPL3-Cloud Policy Framework“ erfüllen

Updated ISPL2 Cloud Security Guideline


ERGO

Cloud Security
ISPL2

Contents

ISPL2_Cloud_S
curity_v1.0_EN.pd

Updated ISPL3 Cloud Policy Framework


ERGO

Cloud Policy Framework
ISPL3
Table of contents

ISPL3_Cloud_S
curity_v1.0_EN.pd

Holistic and risk-based Cloud Framework

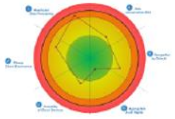
1 Align ISPL2 Cloud Security

- Update existing ISPL2 cloud guideline to updated principles
- Enrich ISPL2 cloud guideline with better practices

2 Align ISPL3 Cloud Policy Framework

- Update existing ISPL3 in line with updated ISPL2
- Enrich ISPL3 with better practices

Risk-based Approach

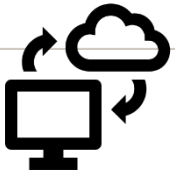


- Build basis for risk-based cloud initiative decisions based on MunichRE approach
- Align evaluation with international standards, e.g. ISO

Initial Control Catalogues

- Use initial Control Catalogue for evaluation of Cloud services
- Align Control Catalogue with better practices

Praktische Erfahrungen mit Cloud-Principles und CGP



Pro:

- Hohe Rechtssicherheit
- Technisch „saubere“ und sichere Lösungen
- Informierte Entscheidungen durch den Vorstand möglich

Con:

- „Hoher Formalismus“ / Aufwand für Prozess Owner und Stakeholder
- Zeitliche Verzögerungen
- Herausforderung bei agilen Projekten

Erfahrungen aus der Praxis bei Umsetzung der rechtlichen Anforderungen

ERGO

- **Die Vorstellungen über die Umsetzung der rechtlichen Anforderungen gehen zwischen ERGO und Cloud-Dienstleister teilweise auseinander.**
- **Insbesondere Dienstleister aus den USA / mit einer US-amerikanischen Konzern-Mutter (z.B. AWS, Microsoft, Salesforce) präferieren weniger strenge / ausführliche Regelungen.**
- **Hierbei stellen insbesondere die den Cloud-Diensten zugrunde liegenden globalen Netzwerke und Zugriffsmöglichkeiten die Dienstleister vor Herausforderungen.**
- **Besondere Problemfelder:**
  - **Verpflichtungserklärung nach § 203 StGB - Nennung einer deutschen Strafrechtsnorm, Hinweis auf strafrechtliche Folgen unerwünscht**
  - **Kontrollrechte für interne / externe Prüfer, BaFin – u.a. Vor-Ort-Prüfungen unerwünscht**

    Aktuell: Diskussion / Gedankenaustausch mit BaFin über praktikable Umsetzung (z.B. Sammelprüfungen durch Versicherer bzw. – präferierte Lösung – Zertifikate durch WP-Gesellschaften)

Je größer der Dienstleister, desto schwieriger / länger die Verhandlungen

Die Vision ist es, die Cloud bei ERGO erfolgreich zu etablieren und damit die ERGO erfolgreicher zu machen.

Group Legal: Unsere Aufgabe ist es, diese Vision unter Beachtung aller rechtlichen Anforderungen zu unterstützen und zu ermöglichen.

Vielen Dank für Ihre Aufmerksamkeit!

Thomas Schick
ERGO Group Legal
thomas.schick@ergo.de
+49 211 477 2360

Dank an meine Kollegen Axel Römer und Ralf Geuenich