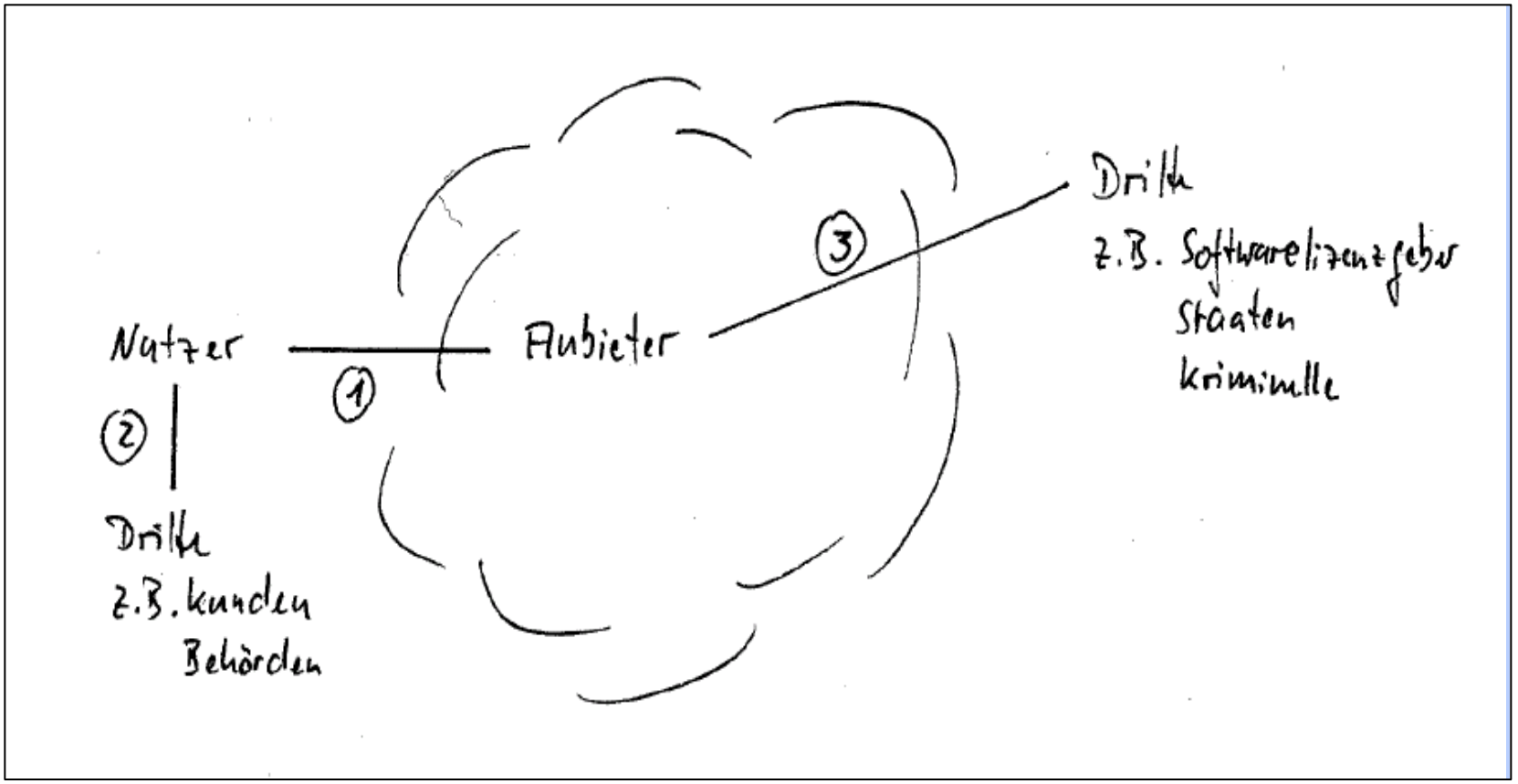
DR. VOCKE & PARTNER
RECHTSANWÄLTE

David Herzog

Rechtliche Rahmenbedingungen des Cloud Computing

„... und wir machen es trotzdem!“

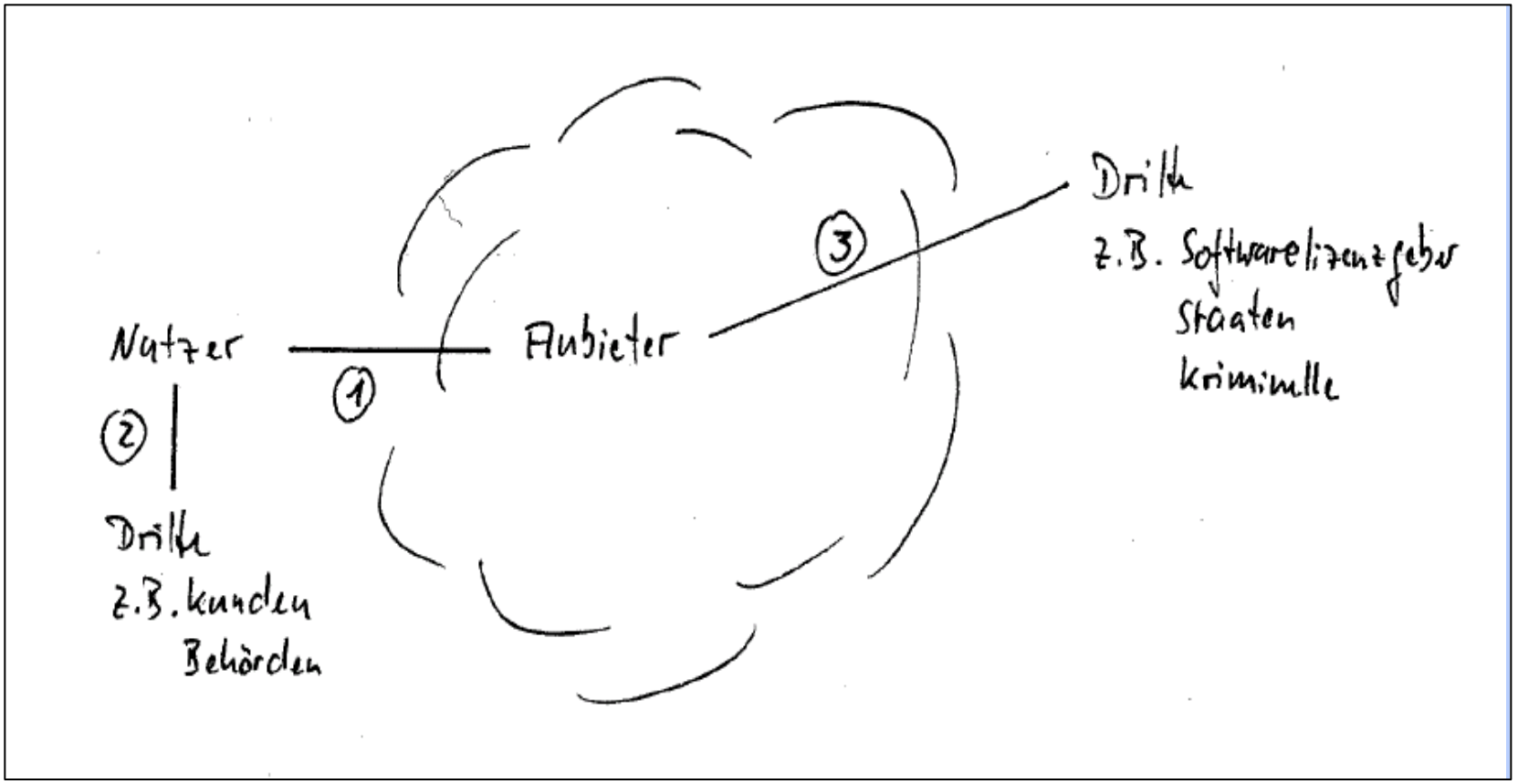
1. Rechtliche Rahmenbedingungen



Verhältnis Nutzer / Anbieter von Cloud-Systemen

- Es gibt keinen gesetzlichen Typenvertrag für Cloud-Systeme.
- Der Schwerpunkt der Rechtsverhältnisse zwischen Nutzer und Anbieter liegt daher im freien vertraglichen Bereich. Zur Anwendung kommen in der Regel Mischverträge, die Elemente des Werkvertrags (§§ 613ff. BGB), des Mietvertrags (§§ 535ff. BGB), des Dienstvertrags (§§ 611ff.BGB) sowie der Leihe (§§ 598ff. BGB) in sich vereinen.
- Außerdem haben sich branchenweit vorgefertigte vertragliche Bedingungen etabliert, die sowohl die Einzelheiten der Leistungserbringung regeln (Service Level Agreements, SLA), als auch die Sicherheit der Datenverarbeitung (Security-Service Level Agreements, SSLA). Diese Bedingungen gleichen sich branchenübergreifend und sind – wegen der Macht des Faktischen - nur in bestimmten Passagen individualisierbar.

1. Rechtliche Rahmenbedingungen



1. Rechtliche Rahmenbedingungen

§ 3 Weitere Begriffsbestimmungen

(1) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) 1Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. 2Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) **Erheben** ist das Beschaffen von Daten über den Betroffenen.

(4) 1**Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. 2Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. **Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

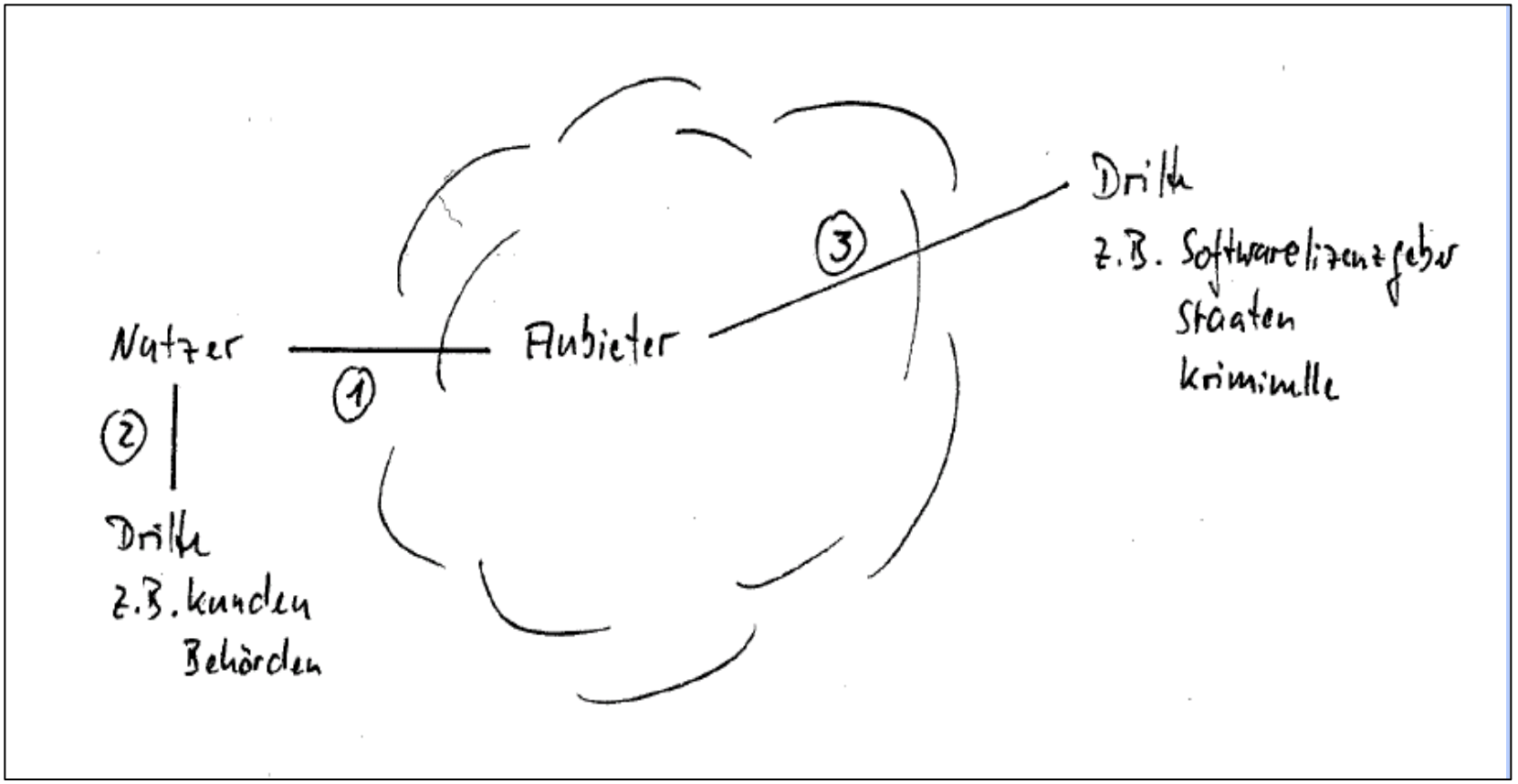
(5) **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

...

(7) **Verantwortliche Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) 1Empfänger ist jede Person oder Stelle, die Daten erhält. 2**Dritter** ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. 3Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten **im Auftrag** erheben, verarbeiten oder nutzen.

1. Rechtliche Rahmenbedingungen



Fragen im Verhältnis zum Anbieter der Cloud-Dienste:

- Erreicht der Anbieter das (Daten)Schutzniveau, das der Nutzer seinen eigenen Kunden schuldet?
- Gewährt der Anbieter im Schadensfall ausreichende Haftung bzw. Haftungsmasse?
- Sind die Ressourcenanbieter als Subunternehmer des Anbieters seriös? Werden ggf. Risiken des Cloud-Anbieters im Rahmen sog. Back-to-Back-Agreements an den Ressourcenanbieter durchgereicht mit der Folge einer Verschlechterung der Regreßmöglichkeiten des Nutzers?
- Kann der Anbieter mit vertretbarem Aufwand juristisch zur Rechenschaft gezogen werden? Das bedeutet: Sind materielles Recht und Prozeßrecht transparent? Kann ein erlangter Vollstreckungstitel am Sitz des Unternehmens überhaupt durchgesetzt werden?
- Kann oder muß eine Auftragsdatenverarbeitung gemäß § 11 BDSG angenommen werden? Achtung: Diese ist gemäß § 3 Abs.8 Satz 3 Halbs.2 BDSG nur innerhalb der EU oder des EWR möglich!

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 - 0050

Artikel 17 Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten **ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist**.

(2) Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.
- Nötige Zusätze individuell vereinbaren, ggf. hilft ein beauty contest mehrere Cloud-Anbieter.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.
- Nötige Zusätze individuell vereinbaren, ggf. hilft ein beauty contest mehrere Cloud-Anbieter.
- Keine personenbezogene Datenverarbeitung ohne Einwilligung oder Dokumentation.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.
- Nötige Zusätze individuell vereinbaren, ggf. hilft ein beauty contest mehrere Cloud-Anbieter.
- Keine personenbezogene Datenverarbeitung ohne Einwilligung oder Dokumentation.
- Keine personenbezogene Datenverarbeitung in der Public Cloud.
  Und in geschlossenen Cloud-Systemen müssen sämtliche Unterauftragnehmer jederzeit bekannt sein, ebenso wie alle Wartungsunternehmen u.ä. Das läßt sich meist nur im Inland abbilden, und verläßlich nur bei ausschließlich deutschen Anbietern. Im Zweifelsfall lassen Sie sich schriftlich bestätigen, daß keine Daten ins Ausland übermittelt oder von dort eingesehen werden können.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.
- Nötige Zusätze individuell vereinbaren, ggf. hilft ein beauty contest mehrere Cloud-Anbieter.
- Keine personenbezogene Datenverarbeitung ohne Einwilligung oder Dokumentation.
- Keine personenbezogene Datenverarbeitung in der Public Cloud.
  Und in geschlossenen Cloud-Systemen müssen sämtliche Unterauftragnehmer jederzeit bekannt sein, ebenso wie alle Wartungsunternehmen u.ä. Das läßt sich meist nur im Inland abbilden, und verläßlich nur bei ausschließlich deutschen Anbietern. Im Zweifelsfall lassen Sie sich schriftlich bestätigen, daß keine Daten ins Ausland übermittelt oder von dort eingesehen werden können.
- Lassen Sie sich periodisch das Datenschutzniveau Ihrer Cloud-Partner schriftlich nachweisen.

3. Best Practice (1 von 2)

- Formularverträge für das Cloud Computing von einem Spezialisten durchsehen lassen. Das ist meist nicht der „Hausanwalt“.
- Nötige Zusätze individuell vereinbaren, ggf. hilft ein beauty contest mehrere Cloud-Anbieter.
- Keine personenbezogene Datenverarbeitung ohne Einwilligung oder Dokumentation.
- Keine personenbezogene Datenverarbeitung in der Public Cloud.
  Und in geschlossenen Cloud-Systemen müssen sämtliche Unterauftragnehmer jederzeit bekannt sein, ebenso wie alle Wartungsunternehmen u.ä. Das läßt sich meist nur im Inland abbilden, und verläßlich nur bei ausschließlich deutschen Anbietern. Im Zweifelsfall lassen Sie sich schriftlich bestätigen, daß keine Daten ins Ausland übermittelt oder von dort eingesehen werden können.
- Lassen Sie sich periodisch das Datenschutzniveau Ihrer Cloud-Partner schriftlich nachweisen.
- Beschäftigen Sie, sobald es geht, einen Compliance-Beauftragten, der sich auch tatsächlich mit dem BDSG und den technischen Rahmenbedingungen des Cloud Computing auskennt.

3. Best Practice (2 von 2)

- Kontrollieren Sie sehr genau, wer was in Ihrem Unternehmen in die Cloud hochladen kann und darf.

3. Best Practice (2 von 2)

- Kontrollieren Sie sehr genau, wer was in Ihrem Unternehmen in die Cloud hochladen kann und darf.
- Richten Sie auch dann ein „Internes Kontrollsystem“ ein, wenn Sie es nicht müssen. Dokumentieren Sie alles. Sie ersparen sich im Zweifelsfall eine Menge Kosten und Ärger.

3. Best Practice (2 von 2)

- Kontrollieren Sie sehr genau, wer was in Ihrem Unternehmen in die Cloud hochladen kann und darf.
- Richten Sie auch dann ein „Internes Kontrollsystem“ ein, wenn Sie es nicht müssen. Dokumentieren Sie alles. Sie ersparen sich im Zweifelsfall eine Menge Kosten und Ärger.
- Lassen Sie sich auch im Vorfeld von Entscheidungen und Streitigkeiten zu einem Zeitpunkt juristisch beraten, an dem Sie noch die Entscheidungsoptionen in der Hand haben.

3. Best Practice (2 von 2)

- Kontrollieren Sie sehr genau, wer was in Ihrem Unternehmen in die Cloud hochladen kann und darf.
- Richten Sie auch dann ein „Internes Kontrollsystem“ ein, wenn Sie es nicht müssen. Dokumentieren Sie alles. Sie ersparen sich im Zweifelsfall eine Menge Kosten und Ärger.
- Lassen Sie sich auch im Vorfeld von Entscheidungen und Streitigkeiten zu einem Zeitpunkt juristisch beraten, an dem Sie noch die Entscheidungsoptionen in der Hand haben.
- Verwenden Sie keine allgemein gebräuchlichen Mobile Devices ungeschützt im Unternehmensbereich. Auch gespeicherte private Mitarbeitertelephonnummern sind bereits personenbezogene Daten.

3. Best Practice (2 von 2)

- Kontrollieren Sie sehr genau, wer was in Ihrem Unternehmen in die Cloud hochladen kann und darf.
- Richten Sie auch dann ein „Internes Kontrollsystem“ ein, wenn Sie es nicht müssen. Dokumentieren Sie alles. Sie ersparen sich im Zweifelsfall eine Menge Kosten und Ärger.
- Lassen Sie sich auch im Vorfeld von Entscheidungen und Streitigkeiten zu einem Zeitpunkt juristisch beraten, an dem Sie noch die Entscheidungsoptionen in der Hand haben.
- Verwenden Sie keine allgemein gebräuchlichen Mobile Devices ungeschützt im Unternehmensbereich. Auch gespeicherte private Mitarbeitertelephonnummern sind bereits personenbezogene Daten.
- Beachten Sie diese Grundsätze auch bei der Entwicklung und Verwendung von Unternehmens- und Business-Apps!

DR. VOCKE & PARTNER
RECHTSANWÄLTE

David Herzog

Vielen Dank für Ihre Aufmerksamkeit.