KPMG

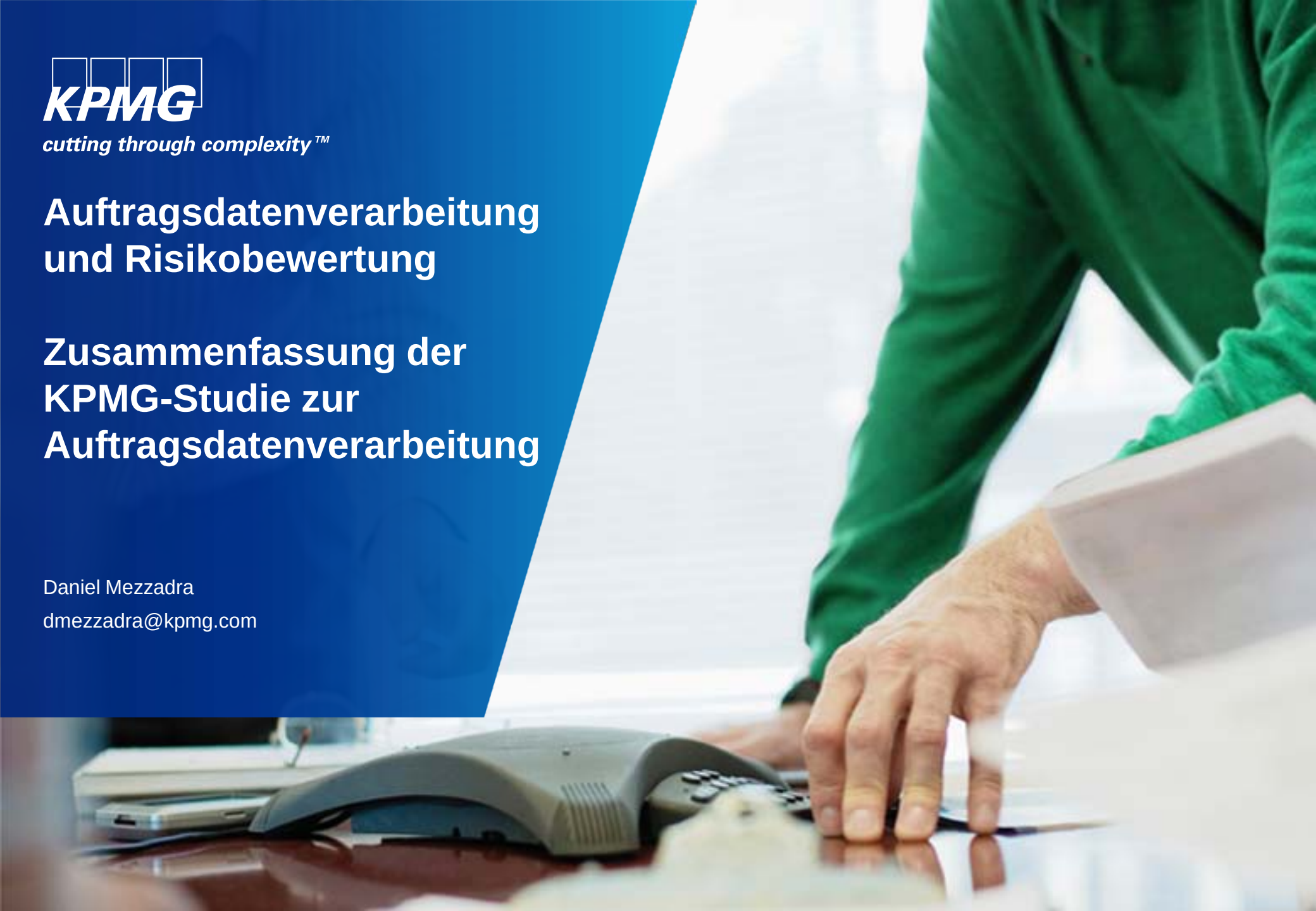
cutting through complexity™

Auftragsdatenverarbeitung und Risikobewertung

Zusammenfassung der KPMG-Studie zur Auftragsdatenverarbeitung

Daniel Mezzadra

dmezzadra@kpmg.com

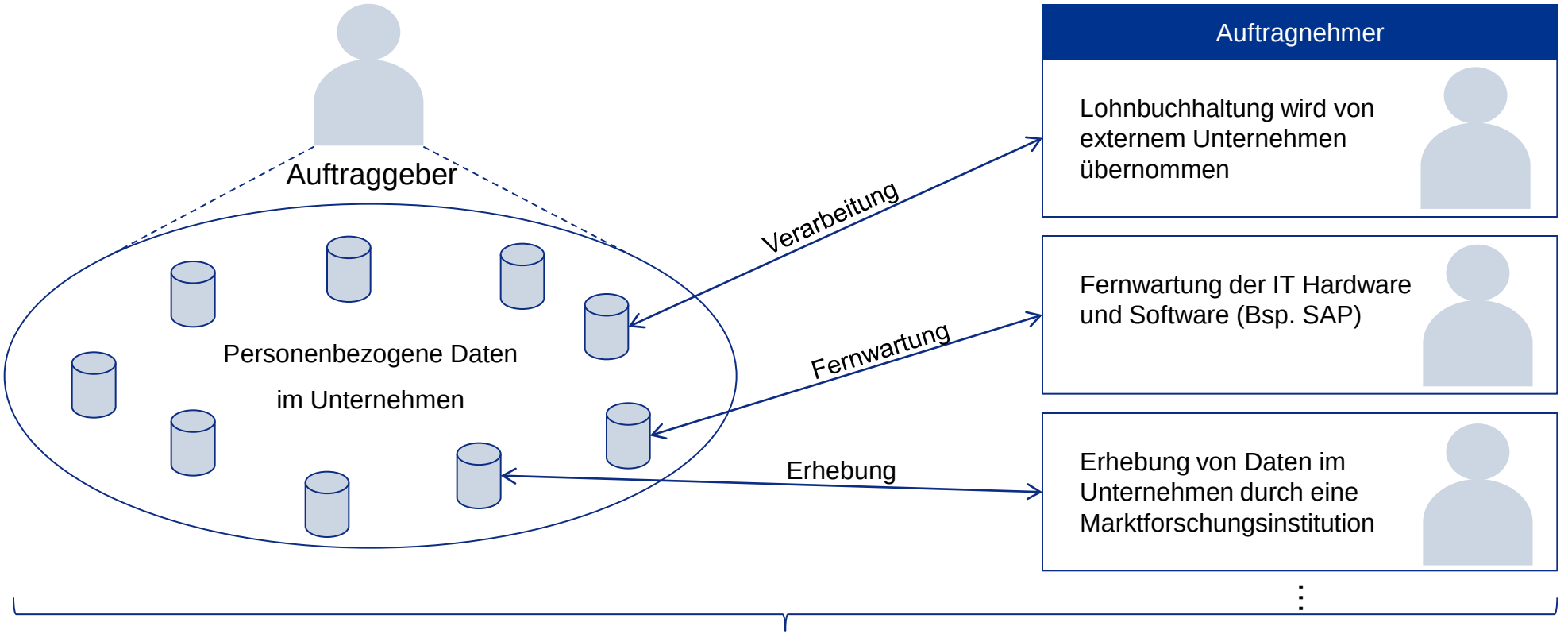


Agenda

Studie zur Auftragsdatenverarbeitung

- **I** Zielsetzung der Studie
- **II** Fragenkatalog
- **III** Auswahl und Methodik
- **IV** Ergebnisse

Was ist Auftragsdatenverarbeitung?



Auftragsdatenverarbeitung liegt vor,
wenn ein Unternehmen (sog. **Auftraggeber**) ein anderes Unternehmen (sog. **Auftragnehmer**) damit beauftragt, **personenbezogene Daten** im Auftrag für das Unternehmen **zu verarbeiten, zu erheben oder zu nutzen**.

Ausgangssituation & Ziele der Studie

Ausgangssituation / Herausforderung

- Mit Inkrafttreten der zweiten Datenschutznovelle am 1. September 2009 ist die Auftragsdaten-verarbeitung (ADV) stärker reguliert
- Zentraler Aspekt ist die gestiegene Verantwortung des Auftraggebers in folgenden Bereichen:
  - Schriftlichen Vertrag mit zwingend in § 11 Abs. 2 BDSG vorgeschriebenen **Mindestinhalten**
  - Sorgfältige Auswahl des Dienstleisters
  - Überprüfung der **technischen und organisatorischen Sicherheitsmaßnahmen** vor Beginn und sodann regelmäßig
- Keine Vorgaben zur Umsetzung der Dokumentation
- Kein genauer Kenntnisstand über den Umgang der Unternehmen mit den neuen Anforderungen

Ziele

- Stimmungsbild erheben
- Informationen erheben über:
  - **Erfüllung** der inhaltlichen und zeitlichen Verantwortung
  - Häufigkeit & Regelmäßigkeit von **Aktivitäten zur Überprüfung**
  - Subjektive **Einschätzung** der Datensicherheit
  - Arten und Umfang der **Dokumentation** von ADV-Verhältnissen
  - Kontrollmaßnahmen der **Datenschutzbehörden**

Agenda

Studie zur Auftragsdatenverarbeitung

- **I** Zielsetzung der Studie
- **II** Fragenkatalog
- **III** Auswahl und Methodik
- **IV** Ergebnisse

Fragenkatalog
Drei zentrale Informations-Aspekte

Bewusstsein über die neuen Anforderungen

- Erhebung, Inwieweit den Unternehmen die Anforderungen der neuen Regelung in § 11 BDSG **bekannt** sind
- Informationen über den **Umfang der Auftragsdatenverarbeitung** erheben
- Umfang ca. 20 % der Fragen

Umgang mit den neuen Anforderungen

- Erkenntnisse darüber gewinnen, **wie** die Unternehmen mit der gestiegenen zeitlichen und inhaltlichen Verantwortung **umgehen**
- Informationen über bestehende **Richtlinien und Prozesse zur Erfüllung** der Anforderungen bei Auftragsdatenverarbeitung erheben
- Informationen über die **Erfüllung der technischen und organisatorischen Maßnahmen** gewinnen
- Umfang ca. 60 % der Fragen

Zielbild und Einschätzung

- Erhebung der **subjektiven Einschätzung über** die inhaltliche und zeitliche **Erfüllung** der Anforderungen sammeln
- Subjektive Einschätzung über die **Bedeutung** des § 11 BDSG und der Auftragsdatenverarbeitung sammeln
- Umfang ca. 20 % der Fragen

Fragenkatalog
2 separate Fragebögen für Auftragnehmer und Auftraggeber

Fragebogen Auftragnehmer

- Bewusstsein über Auskunftsrecht der Auftraggeber erfassen
- Information über die Qualität und Quantität von ADV-Verhältnissen und den Umfang der Nachfrage der Auftraggeber
- Subjektive Einschätzung der Situation

Fragebogen Auftraggeber

- Bewusstsein über die gestiegene Verantwortung durch § 11 BDSG erfassen
- Aktueller Umgang mit den gestiegenen Anforderungen
- Informationen über Nachfragen der Datenschutzbehörden
- Subjektive Einschätzung der Situation

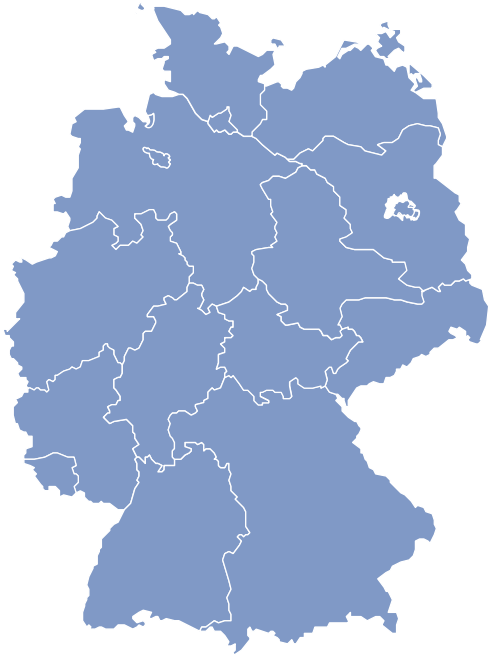
Die Studie erhebt auch die Sichtweise der Auftragnehmer

Agenda

Studie zur Auftragsdatenverarbeitung

- **I** Zielsetzung der Studie
- **II** Fragenkatalog
- **III** Auswahl und Methodik
- **IV** Ergebnisse

Telefonische Befragung und ergänzende Fragebögen



Studienansatz

- Ziel: mind. **>50 Auftragnehmer** und **>50 Auftraggeber** mit vorhandener Auftragsdatenverarbeitung zu befragen
- **Telefoninterview** mit den Datenschutzbeauftragten der jeweiligen Unternehmen
- Unternehmen aus den **Sektoren**: Banken, Leasing, Inkasso, Zahlungsabwickler , IT-Dienstleister für Finanzinstitute
- Beschränkung auf in **Deutschland** ansässige Unternehmen

Methode der Erhebung: Telefonische Befragung und Fragebögen bei Bedarf

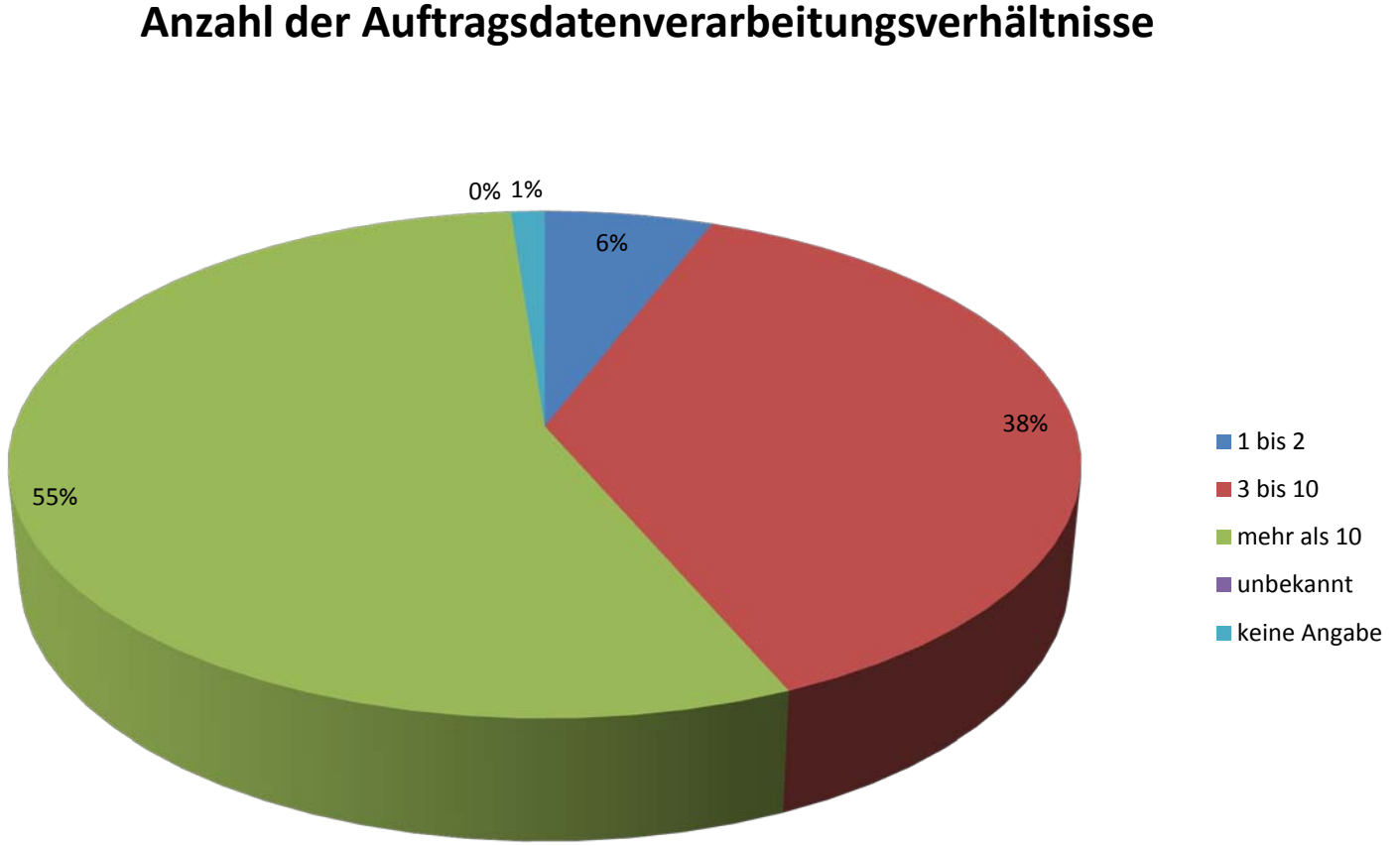
Agenda

Studie zur Auftragsdatenverarbeitung

- **I** Zielsetzung der Studie
- **II** Thesen & Fragenkatalog
- **III** Auswahl und Methodik
- **IV** Ergebnisse

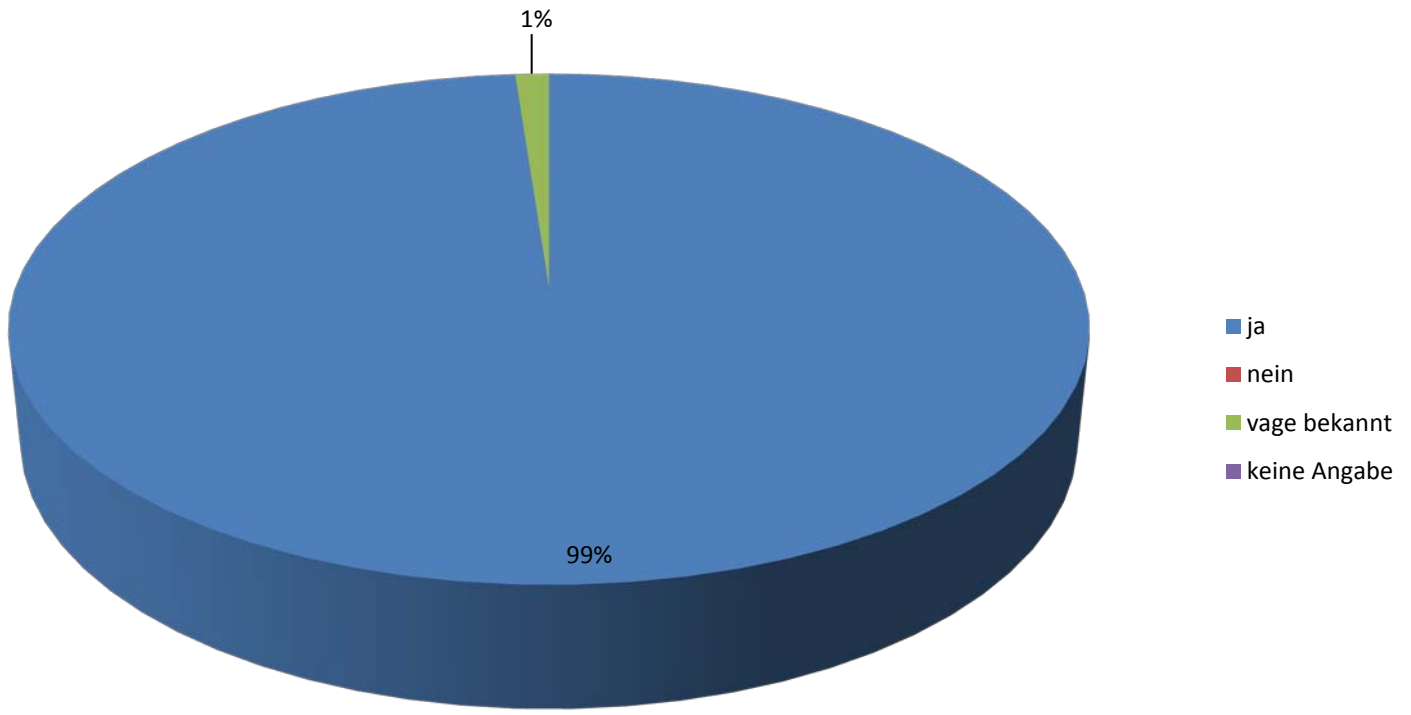
Anzahl der Auftragsdatenverarbeitungsverhältnisse (ADV)

Über die Hälfte der befragten Unternehmen verfügt über mehr als 10 Auftragsdaten-verarbeitungs-verhältnisse



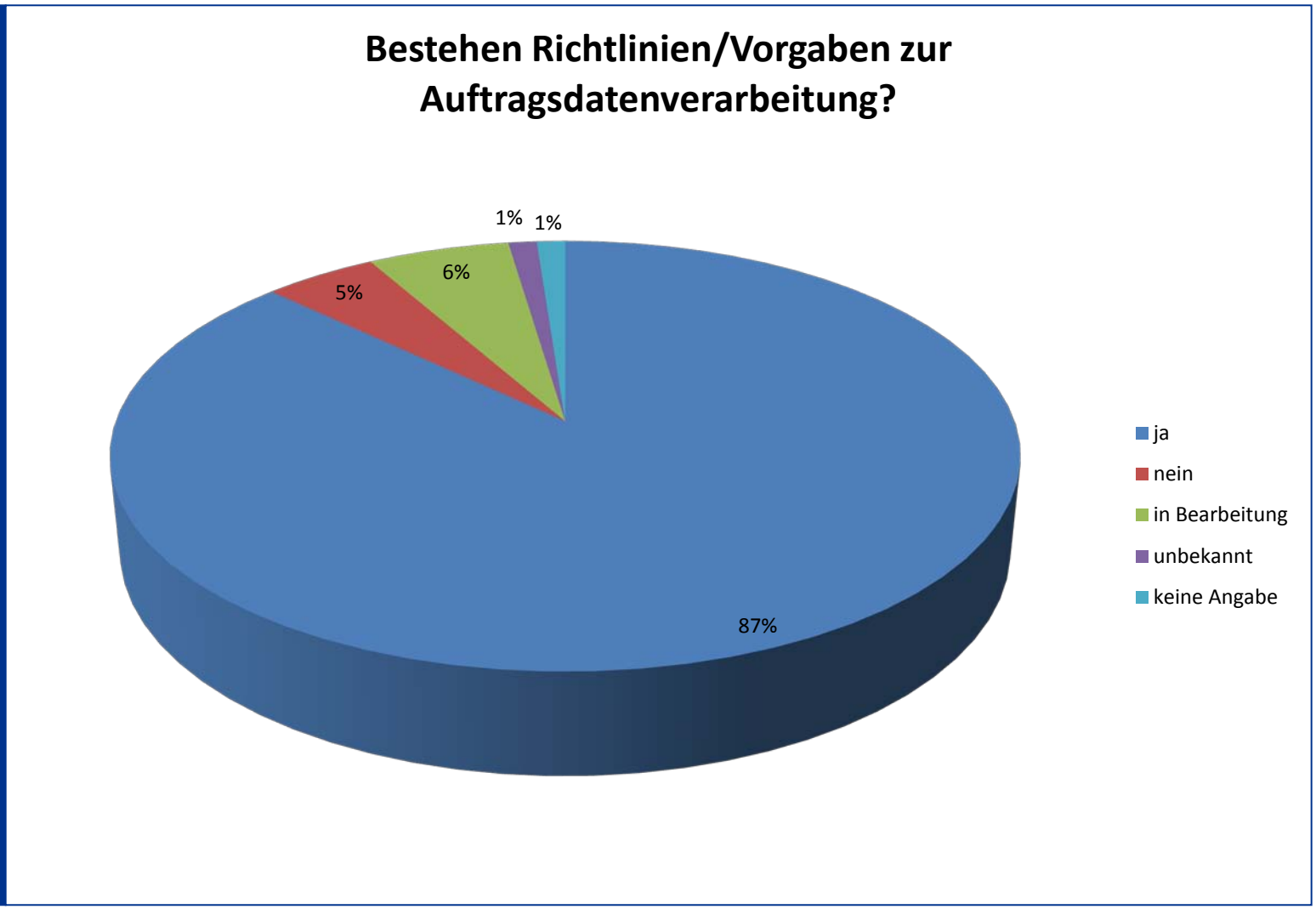
Bewusstsein über gestiegene ADV-Verantwortung

Fast allen Datenschutz-beauftragten (99%) ist die Novellierung des § 11 BDSG bekannt



Richtlinien und Vorgaben zur Auftragsdatenverarbeitung (ADV)

87 Prozent der befragten Unternehmen haben bereits Richtlinien/ Vorgaben zur ADV erstellt

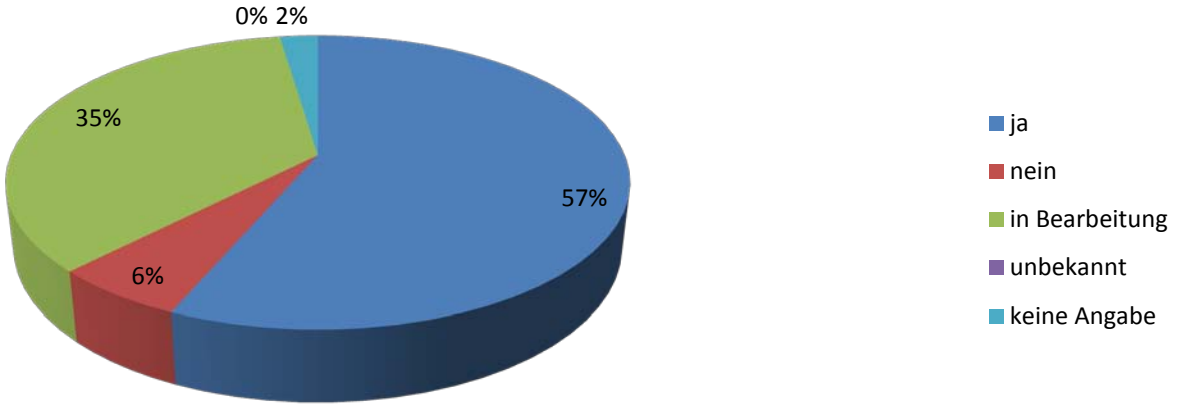


Inventarisierung der Auftragsdatenverarbeitungsverhältnisse (ADV)

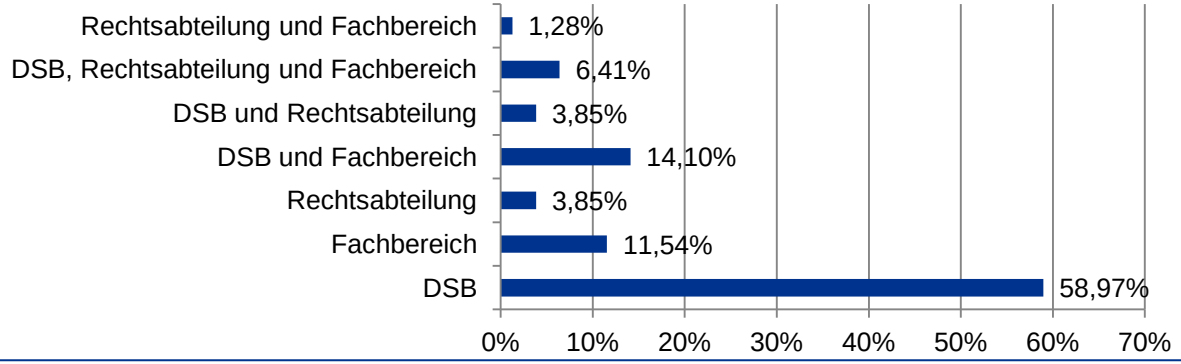
Über die Hälfte (57 %) der befragten Unternehmen hat bereits ein vollständiges Inventar

Bei rund einem Drittel ist dies in Bearbeitung (35 %)

Ist bereits ein Inventar erstellt?

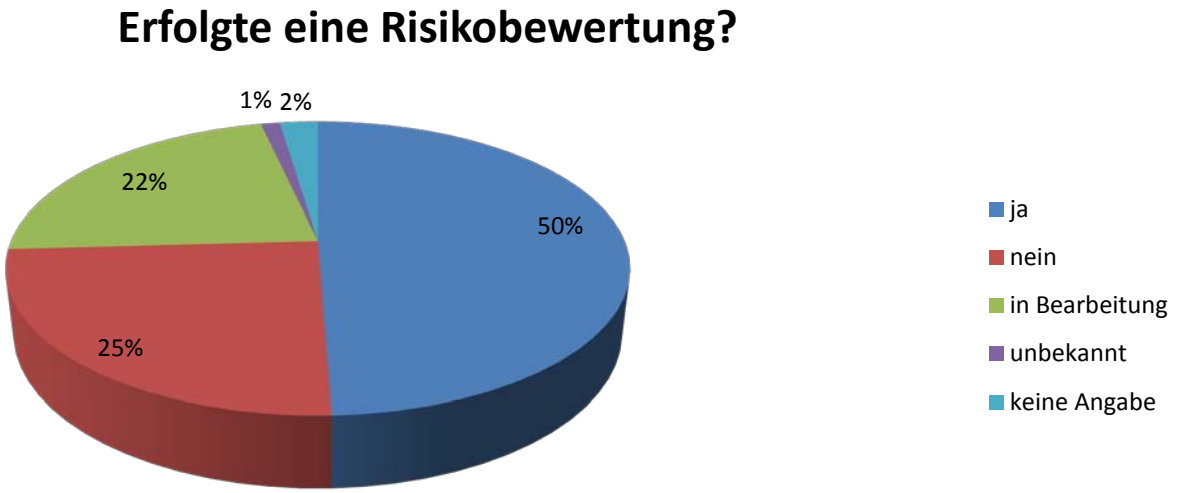


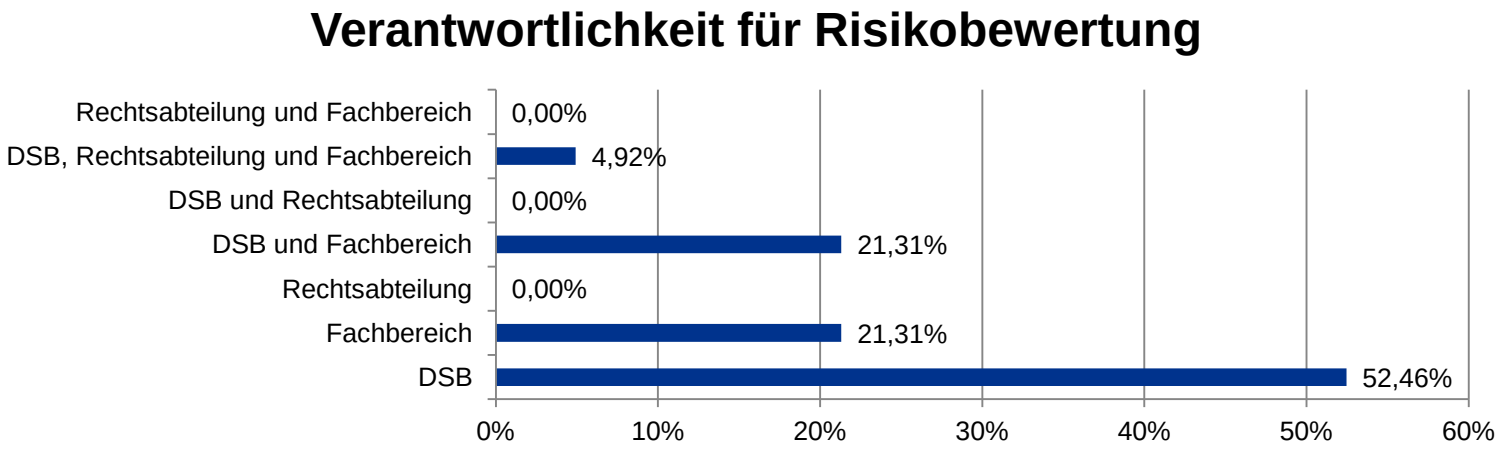
Verantwortlichkeit für das Erstellen des Inventars



Risikobewertung der Auftragsdatenverarbeitungsverhältnisse (ADV)

25 Prozent der befragten Unternehmen führen keine Risiko-bewertung für ADV durch

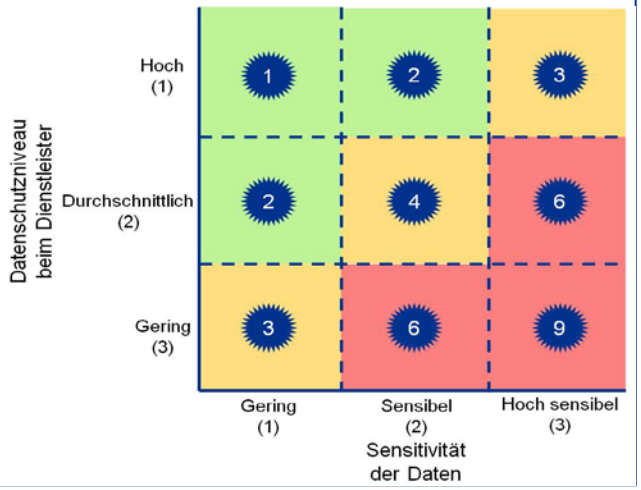




Exkurs: Risikobewertung der Auftragsdatenverarbeitungsverhältnisse

Alle ADV-Verhältnisse sollten in eine Risikomatrix eingeordnet werden.

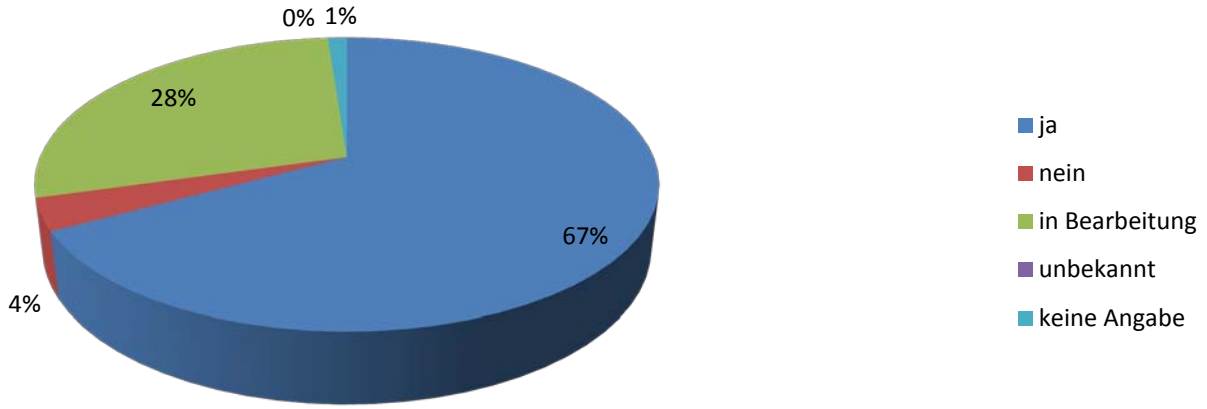
- Für jedes ADV-Verhältnis sollte mindestens einmal jährlich eine **Risikobewertung** durchgeführt werden. Jedes ADV-Verhältnis ist dabei anhand von verschiedenen Risikokriterien zu bewerten, um auf dieser Basis angemessene Maßnahmen zur Erfüllung der Anforderungen des § 11 Abs. 2 BDSG zu genügen.
- Für eine einheitliche und effiziente Risikobewertung bieten sich die Kriterien **Sensitivität der Daten** und **Datenschutz-Niveau des Dienstleiste**rs an.
- Abhängig vom Ergebnis der Risikobewertung des ADV-Verhältnisses gemäß Risikomatrix sollten zur Erfüllung der Anforderungen des § 11 Abs. 2 BDSG **abgestufte Maßnahmen** ergriffen werden



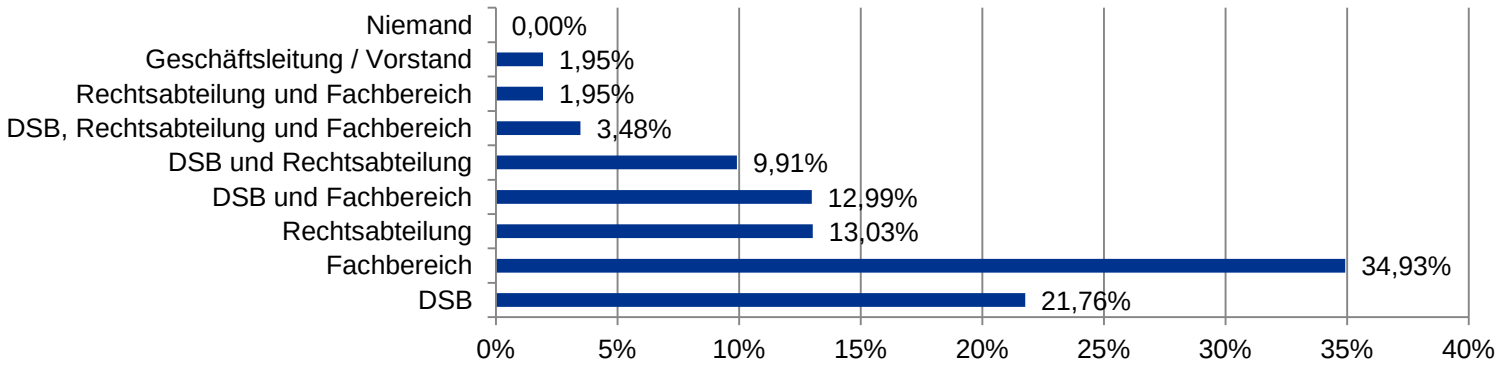
Anpassung der ADV-Verträge

Die Mehrheit der befragten Unternehmen hat die Verträge mit den Auftrag-nehmern bereits angepasst (67%) oder ist gerade dabei dies zu tun (28%)

Sind die Verträge bereits angepasst?



Verantwortlichkeit bei Vertragsanpassung



Exkurs: Möglichkeiten der Überprüfung der technische und organisatorische Maßnahmen

Überprüfung der TOMs	+ Vorteile	- Nachteile
Fragebögen	▪ Für wenig sensible ADV-Verhältnisse mit weiteren Nachweisen gut anwendbar	▪ Keine unabhängige Aussage oder Prüfung ▪ Aufwand steigt mit Anzahl der ADV-Verhältnisse (AN)
Sicherheits-Richtlinien einsehen	▪ Für wenig sensible ADV-Verhältnisse mit weiteren Nachweisen gut anwendbar	▪ Keine Aussage/Sicherheit zur Umsetzung und Anwendung der Richtlinie
Eigene Vor-Ort-Prüfung	▪ Hohe Verlässlichkeit ▪ Prüfung auf Umsetzung und Wirksamkeit von Kontrollen	▪ Hoher Aufwand bei AG und AN, insbesondere bei steigender Anzahl von ADV-Verhältnissen
Prüfungsbericht der internen Revision	▪ Prüfung auf Umsetzung und Wirksamkeit von Kontrollen	▪ I.d.R. keine vollständige Betrachtung der Anforderungen ▪ Keine unabhängige Aussage bzw. Prüfung
Prüfung durch Externe	▪ Mittlere Verlässlichkeit ▪ Prüfung auf Umsetzung und Wirksamkeit von Kontrollen	▪ Basieren häufig nicht auf allgemein zugänglichen Standards (wie beispielsweise ISO 27001) ▪ Keine ausreichende Transparenz über durchgeführte Prüfungshandlungen
Prüfung nach anerkanntem Prüfungsstandard	▪ Unabhängige Aussage zur Umsetzung und Wirksamkeit ▪ Hohe Verlässlichkeit und Nachhaltigkeit durch Transparenz zu DS-IKS und zu Prüfungshandlungen ▪ Für Mehrmandanten-Dienstleister anwendbar	▪ Bei geringer Anzahl der ADV-Verhältnisse kein Leverage (AN) ▪ ISAE 3000 außerhalb des Finanzbereiches noch wenig bekannt

Exkurs: Anerkannter Prüfungsstandard ISAE 3000

ISAE 3000: Assurance Engagements other than Audits or Reviews of historical financial Information

- Der Prüfungsstandard ISAE 3000 wurde von der International Federation of Accountants (**IFAC**), dem internationalen Dachverband der Wirtschaftsprüfer, erarbeitet und ist weltweit bekannt und anerkannt.
- Der Prüfungsstandard ISAE 3000 legt u.a. **Mindestanforderungen** an die Unabhängigkeit, an die Prüfungsplanung, -durchführung und -dokumentation sowie an die Qualitätssicherung fest.
- §11-Berichte umfassen zwei wesentliche Aspekte:
  - Beurteilung der **Wirksamkeit des datenschutzrelevanten internen Kontrollsystems** gem. internationalem Rahmenwerk „Internal Control – Integrated Framework“ des Committee of Sponsoring Organizations of the Treadway Commission (COSO).
  - Darstellung und Beurteilung der wesentlichen umgesetzten **Maßnahmen** für die in Anlage zu § 9 BDSG genannten Anforderungen.

Exkurs: Datenschutzrelevantes internes Kontrollsystem

Elemente des datenschutz-relevanten internen Kontroll-systems

- **Kontrollumfeld**
  Die innerbetriebliche Organisation muss insgesamt so gestaltet sein, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
- **Risikobewertung**
  Das Unternehmen sollte eine Risikobetrachtung der bei ihm verarbeiteten personenbezogenen Daten vorgenommen haben.
- **Information uns Kommunikation**
  Die mit der Verarbeitung von personenbezogenen Daten betrauten Personen müssen mit den Vorschriften des BDSG sowie anderen Vorschriften über den Datenschutz vertraut gemacht worden sein.
  Die Geschäftsleitung sollte vom Datenschutzbeauftragten regelmäßig über die datenschutzrelevanten Risiken und implementierten Datenschutzmaßnahmen informiert werden.
- **Überwachung**
  Der Datenschutzbeauftragte sollte regelmäßig sowohl anlassbezogene als auch laufende Überwachungsmaßnahmen im Unternehmen durchführen.

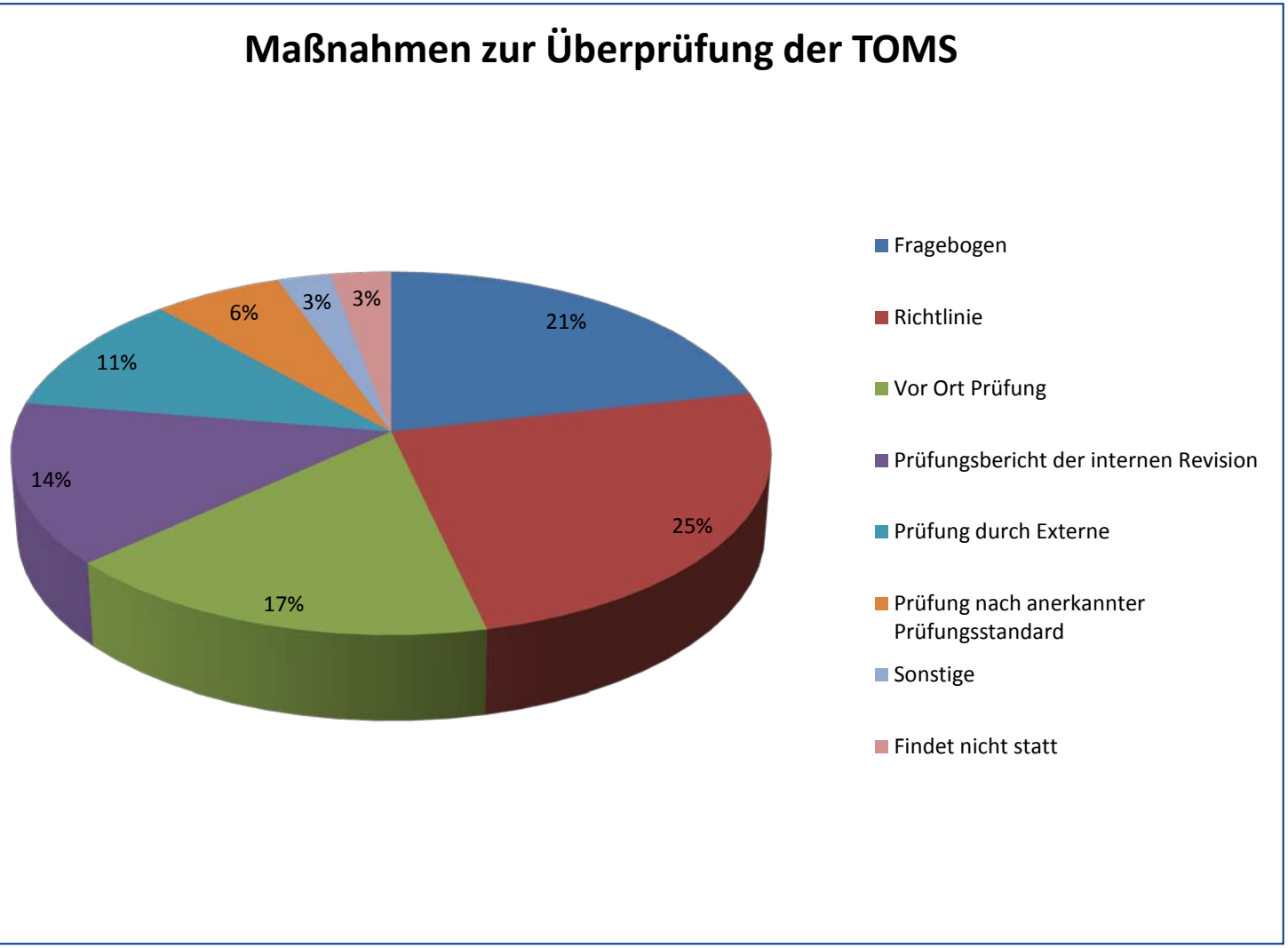
Exkurs: Darstellung der umgesetzten Maßnahmen und deren Prüfung

Transparente Darstellung der wesentlichen Umsetzungsmaßnahmen der in Anlage zu § 9 BDSG genannten Anforderungen und deren Prüfung

Kontrollziel 1		
Angemessene technische und organisatorische Maßnahmen sollen gewährleisten, dass Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen haben, mit denen personenbezogene Daten verarbeitet oder genutzt werden (Zutrittskontrolle).		
Kontroll-ID	**Kontrollbeschreibung erstellt [redacted]**	**Prüfungshandlungen und Prüfungsergebnisse durch KPMG**
1.01	Die Räumlichkeiten in beiden Rechenzentren sowie die Geschäftsräume sind in verschiedene Sicherheitszonen unterteilt. Die Gelände sind umzäunt sowie durch Kamera[illegible] überwachung, Einbruchmeldeanlage und ele[illegible]n Übersteigeschutz gesichert. Wachpersonal und elektronische [illegible]ser kontrollieren die Einhaltung der Zu[illegible]te zu den Sicherheitszonen.	**Prüfungs[illegible]andlungen** Befr[illegible]g des Managements nach Ar[illegible] Umfang des Prozesses um [illegible]e Angemessenheit der Kontrolle zu bestimmen. Einsichtnahme in die Prozessbeschreibungen, um sicherzustellen, dass Kontrollen angemessen definiert und dokumentiert sind. Begehung der Rechenzentren und Geschäftsräume, um die implementierten Kontrollen zu beobachten. **Prüfungsergebnis** Keine Beanstandungen.

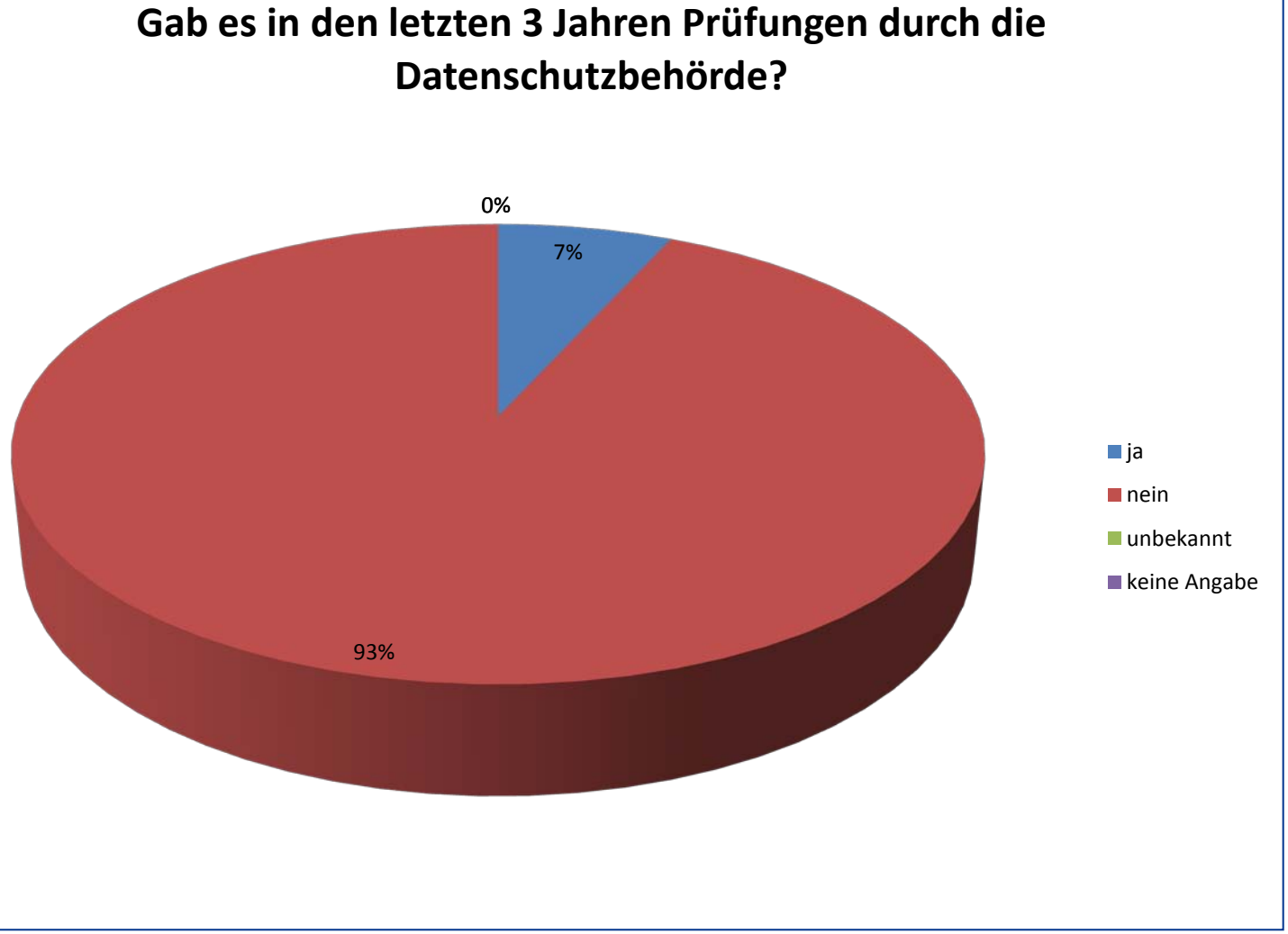
Überprüfung der technische und organisatorische Maßnahmen

Einholen von Prüfungs-berichten nach einem anerkannten Prüfungs-standard erfolgte erst in 6 Prozent aller Fälle



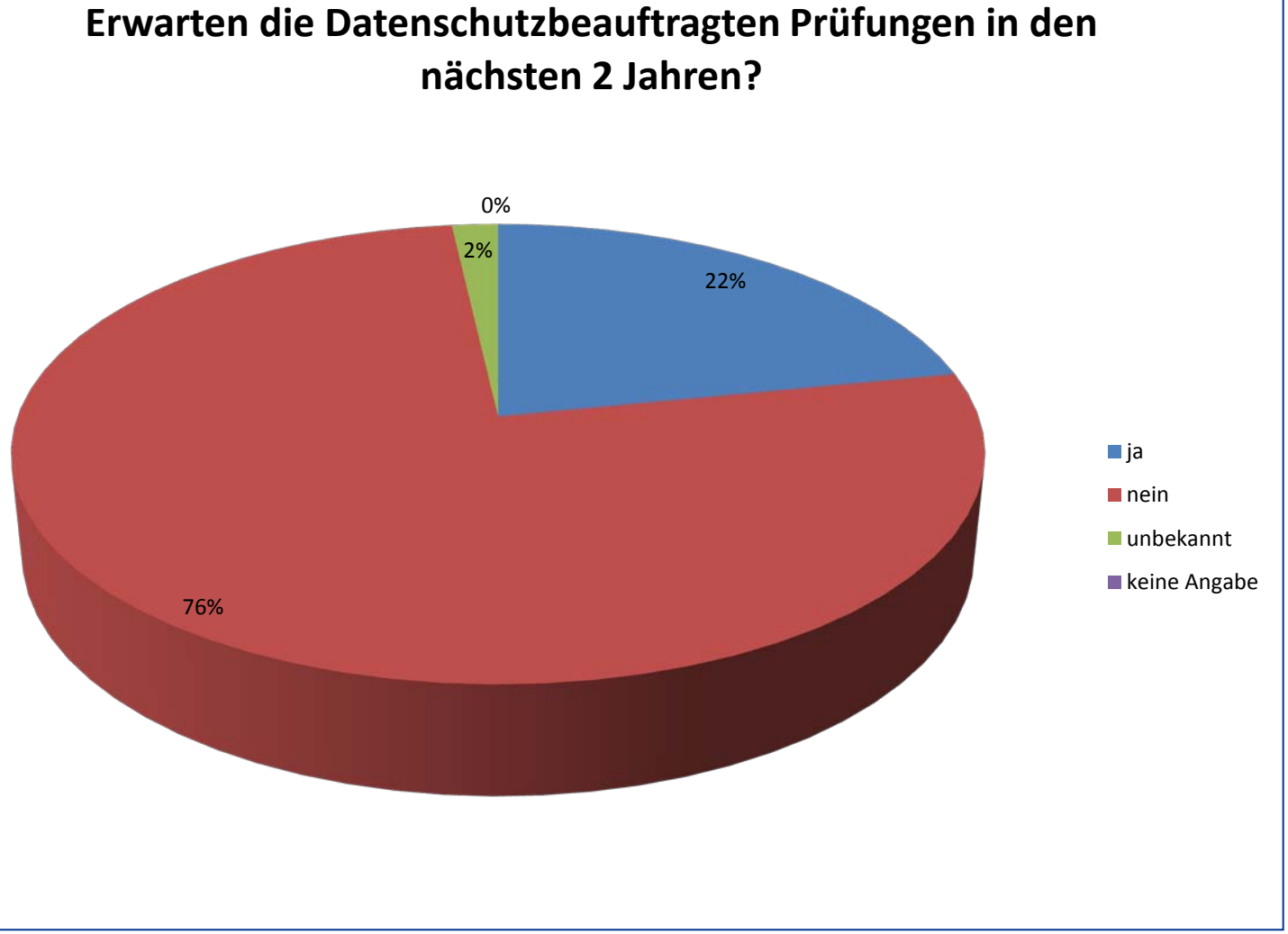
Aktivität der Datenschutzbehörden

Nur 7 Prozent der befragten Unternehmen gaben an, dass in den letzten drei Jahren eine Prüfung durch eine Datenschutz-behörde stattgefunden hat



Aktivität der Datenschutzbehörden

Knapp ein Viertel (22 %) der befragten Datenschutz-beauftragten rechnet mit einer Prüfung der Datenschutz-behörden in den nächsten zwei Jahren



Drei Kernaussagen

Aktivitäten begonnen, aber zu wenig risiko-orientiert

- Viele Unternehmen haben bereits die Auftragsdatenverarbeitungsverhältnisse **inventarisiert**, die **Verträge angepasst** und eine **Richtlinie** zur Auftragsdatenverarbeitung **erstellt**.
- Eine **Risikobewertung** der identifizierten Auftragsdatenverarbeitungsverhältnisse haben jedoch nur rund 30 Prozent der befragten Unternehmen vorgenommen.

Geforderte Überprüfung findet uneinheitlich statt

- Für die vom Gesetzgeber geforderte Überprüfung der Einhaltung der technischen und organisatorischen Maßnahmen haben sich verschiedene Verfahren etabliert, die von intern und extern durchgeführten Vor-Ort-Prüfungen über Dokumentenreviews bis hin zu einfachen Abfragen reichen.
- **Prüfungsberichte** nach anerkannten Prüfungsstandards (u.a. ISAE 3000) wurden erst in geringem Umfang genutzt.

Geringe Aktivitäten durch die Datenschutz-behörden

- Die Datenschutzbehörden haben bei den befragten Unternehmen in der Regel keine Datenschutzprüfungen seit Novellierung des BDSG durchgeführt. Viele Unternehmen stehen aber in **aktivem Austausch mit den Datenschutzbehörden**.
- Ein Viertel der befragten Datenschutzbeauftragten erwartet jedoch in den nächsten zwei Jahren eine **Prüfung durch die Datenschutzbehörden**.

Schlussfolgerungen

Fazit

- Als Gesamtergebnis der Studie lässt sich festhalten, dass die Unternehmen zur Vermeidung von Bußgeldern und Reputationsschäden mit gravierenden Auswirkungen auf den Geschäftserfolg das Thema Auftragsdatenverarbeitung **noch gezielter angehen** müssen.
- DieAuftragsdatenverarbeitungsverhältnisse müssen **risikoorientiert klassifizieren** werden**.** Dazu sind sowohl die Sensitivität der personenbezogenen Daten als auch das Schutzniveau des Dienstleisters zu berücksichtigen.
- Bei **sensiblen Auftragsdatenverarbeitungsverhältnissen** darf sich der Auftraggeber nicht ausschließlich auf Aussagen des Auftragnehmers verlassen, sondern muss eigene Vor-Ort Prüfung durchführen oder einen Bericht nach anerkanntem Prüfungsstandard einfordern.
- Als Grundlage für die notwendige Sicherheit in der Zusammenarbeit zwischen Unternehmen bietet sich ein Prüfungsbericht nach dem internationalen Prüfungsstandard ISAE 3000 an, der den Anforderungen der Auftragsdatenverarbeitung entsprechend über das **datenschutzrelevante Kontrollsystem** und die **Angemessenheit der nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen** transparent berichtet.

Daniel Mezzadra
Manager
Information Risk Management
+49 69 9587-2756
dmezzadra@kpmg.com

Weitere Informationen

Weitere Literatur zu diesem Thema:

Datenschutz und Datensicherheit 6/2011

KPMG Studie zur ADV 2012

cutting through complexity™