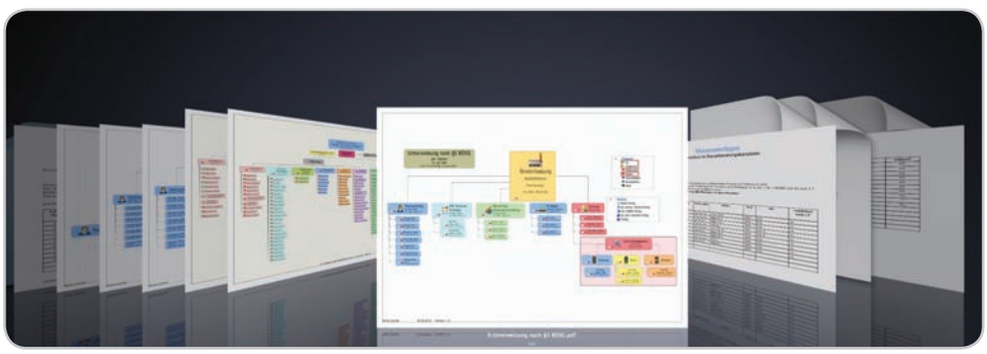
# II Einführung

*Von der Erfahrung anderer profitieren*

Wäre es nicht interessant, wenn Sie in der Datenschutz-Dokumentation eines anderen Unternehmens stöbern könnten? Sich ansehen könnten, wie der Tätigkeitsbericht oder die Verfahrensübersicht aussieht? Wenn Sie dann noch wüssten, dass mehrere Unternehmen diese Dokumentation über Jahre hinweg erfolgreich nutzen – würden Sie nicht unbedingt einen Blick hineinwerfen wollen?

Beim Blättern in einem solchen Ordner fänden Sie vielleicht Organigramme, grafische Übersichten und Flussdiagramme, die Sie mit ein paar kleinen Änderungen für Ihre Datenschutzarbeiten nutzen könnten.



*Beispiel für ein übersichtliches Organigramm*

Man müsste nur wissen, aufgrund welcher Datenschutzaufgabe diese Grafik entstanden ist und welche Ergebnisse damit erzielt wurden. Auf dieser Grundlage etwas Eigenes für Ihr Unternehmen zu erstellen, wäre auch nicht schlecht!

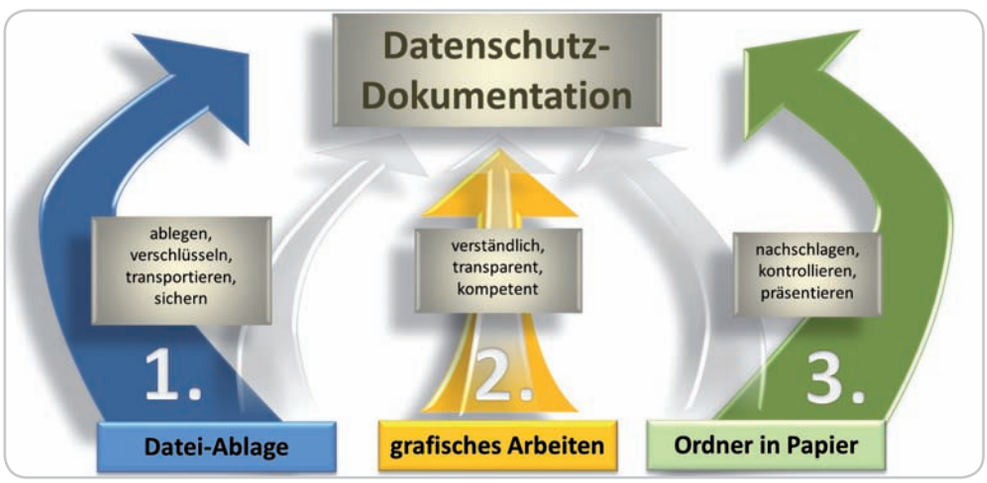

*Etagenübersicht mit bewerteten Sicherheitsbereichen*

Doch was nützen Ihnen all die schönen Informationen, wenn Sie keine bearbeitbaren Dateien dazu bekommen können? Und selbst wenn Sie die Dateien bekämen und keine Lizenzrechte zu beachten wären: Müssten Sie nicht erst zeitaufwendig eine grafische Software erlernen? Da wäre eine kurze Einführung in diese Software perfekt, oder noch besser gleich ein Video von ein bis zwei Minuten Länge, das man auch auf einem iPad schnell als Hilfe aufrufen kann.

# II.1 Was erwartet Sie in diesem Buch?

Stellen Sie sich vor, dass dieses Buch die Rolle einer solchen umfassenden Datenschutz-Dokumentation erfüllt und all Ihre Vorstellungen mit Ihnen gemeinsam umsetzt.

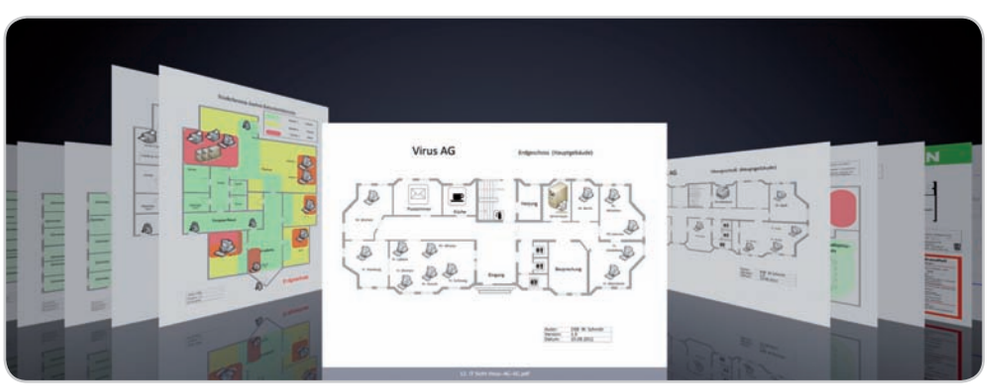
Begleiten Sie mich, wie ich für Sie meine eigene Datenschutz-Dokumentation, die sich in jahrelanger Erfahrung eines externen Datenschutzbeauftragten entwickelt hat, in drei Bereiche zerlege.




*Die drei Bereiche meiner Datenschutz-Dokumentation*

Ich schildere Ihnen, bei welchen Aufgaben ich damit erstaunliche Ergebnisse erzielt habe, wie grafische Darstellungen meine Arbeit als Datenschutzbeauftragter erleichterten und wie dabei meine Anerkennung im Management wuchs.

Folgen Sie meinen Leitfäden von der Beherrschung des Dokumentenchaos zur schnellen und einfachen Erstellung komplexer grafischer Darstellungen bis zur Ermittlung von Verfahren in Ihrer internen Verfahrensübersicht.



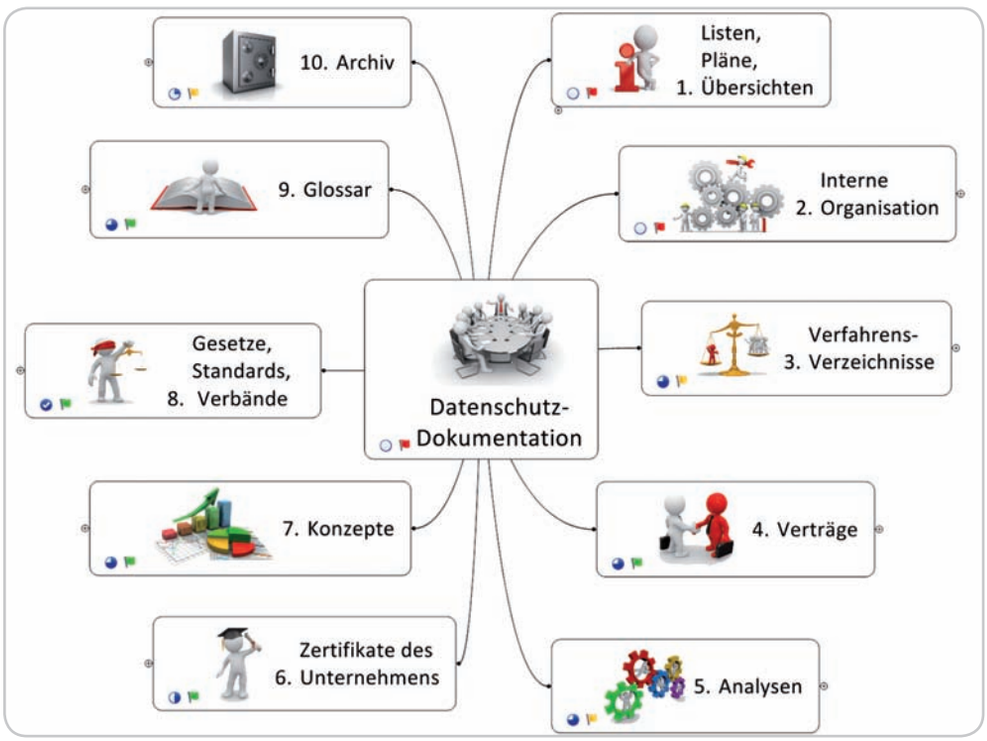

*Grundriss mit IT-Infrastruktur*

Sie werden in jedem Kapitel dieses Buches auf neue Möglichkeiten stoßen, wie Sie Ihre Arbeit als Datenschutzbeauftragter in ein neues Licht rücken können.

*Erstellen Sie Schritt für Schritt Ihre eigene Dokumentation*

Nachdem Sie sich in meiner Datenschutz-Dokumentation einen Überblick über meine Arbeit als externer Datenschutzbeauftragter der letzten Jahre verschafft haben, eröffne ich Ihnen die Möglichkeit, Ihre eigene Datenschutz-Dokumentation Schritt für Schritt zu erstellen. Nutzen Sie meine Erläuterungen als Leitfaden, so haben Sie am Ende Ihre umfassende Datenschutz-Dokumentation vorliegen mit einer digitalen Dateiablage, einer grafi-

schen Schaltzentrale zur Beherrschung des Dokumentenchaos sowie Ihrem Datenschutz-Ordner in Papierform.




*Die grafische Schaltzentrale*

Setzen Sie nur die Methoden, Organigramme, grafischen Listen, Flussdiagramme und Businessgrafiken ein, die für Sie von Vorteil sind, und geben Sie Ihren bisherigen Arbeiten einen Platz in Ihrer neuen Datenschutz-Dokumentation.

*Was hat sich bewährt?*

Anhand meiner eigenen Dokumentation zeige ich Ihnen, was sich an grafischen Übersichten, Plänen und Flussdiagrammen über die Jahre bewährt hat. Ich erläutere an Praxisbeispielen deren Entstehung und die Vorteile, die sich daraus für meine Arbeit als Datenschutzbeauftragter ergeben haben.

*Grafische Tools einfach erklärt*

Ich beschreibe Ihnen ohne große Einführungskurse in einfachen Schritten die Handhabung von grafischen Tools wie MindManager und MS Visio, die ich für meine Darstellungen benutzt habe. Alles so, dass Sie es gleich nachvollziehen können.

Um für Sie den Nutzen noch größer zu machen, werde ich mit Ihnen an vielen Mustern gleich die Anpassung an Ihr Unternehmen vornehmen.

Anhand kleiner Erfahrungsberichte erläutere ich Ihnen, was alles in meinem Datenschutzalltag gut funktioniert hat und an welcher Stelle ich unerwartet Anerkennung für meine Arbeiten als Datenschutzbeauftragter erhalten habe.

*Die Poster*

In der Umschlagklappe finden Sie drei Poster im DIN-A2-Format. Das erste gibt Ihnen einen Überblick über die Grundstruktur Ihrer Datenschutz-Dokumentation, damit Sie sie immer im Blick haben. Das zweite Poster stammt aus meinen Übersichten und zeigt Ihnen alle wichtigen Punkte rund um die technisch-organisatorischen Maßnahmen. Es lässt sich daher auch als Checkliste verwenden. Das Poster ist ein gutes Beispiel dafür, was sich alles mit dem MindManager grafisch darstellen lässt. Das dritte Poster visualisiert, mit wie vielen unterschiedlichen Themen sich ein Datenschutzbeauftragter auseinandersetzen muss.

Ich empfehle den Neueinsteigern unter Ihnen, dieses Buch als Leitfaden für die Arbeit mit und für den Datenschutz zu betrachten. Wer die Datenschutzthemen schon intensiv kennt und bereits mehrere Jahre Datenschutzbeauftragter ist, wird einige neue Anregungen für seine eigene Arbeit mitnehmen können.

# II.2 Was finden Sie auf der CD?

Auf der beiliegenden CD befinden sich vier Verzeichnisse:

1. Muster-Datenschutz-Dokumentation

Im ersten Verzeichnis finden Sie die Struktur meiner Datenschutz-Dokumentation mit allen Dateien, die im Buch besprochen werden, wie bearbeitbaren Plänen, Organigrammen, grafischen Listen oder Konzepten, Mindmap-Dateien, die Sie an Ihre Arbeiten anpassen können und Flussdiagrammen im Visio-Format. Hier entscheiden Sie auch, welche dieser Dateien für Sie von Interesse sind.

2. Ihre Datenschutz-Dokumentation

Das zweite Verzeichnis wird Ihre eigene Datenschutz-Dokumentation. Die Inhalte setzten sich aus drei Komponenten zusammen: Ihren Favoriten und den Dokumenten aus dem ersten Verzeichnis sowie Ihren eigenen Datenschutzunterlagen.

3. Software

Im Verzeichnis „3. Software“ befinden sich Aufrufmöglichkeiten für Softwareprodukte, die in diesem Buch genutzt werden, wie MindManager, MS Visio und Docusnap.

4. Video-Clips

Für einen schnelleren Einstieg in einzelne Themen liegen kurze Video-Clips in diesem Verzeichnis.

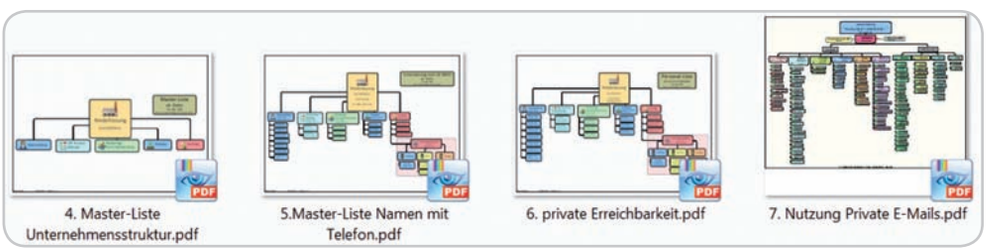
Die Themen sind mit  gekennzeichnet.

*Stöbern Sie auf der CD*

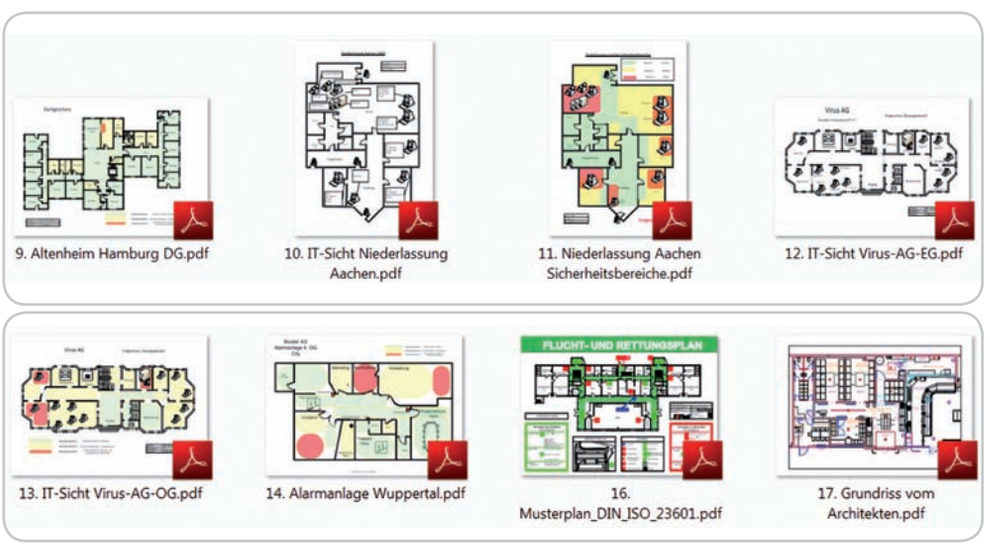
Sollte ich Ihr Interesse geweckt haben, empfehle ich Ihnen, das Buch zur Seite zu legen, auf der CD im Verzeichnis „1. Muster-Datenschutz-Dokumentation“ unter „1. Listen, Pläne, Übersichten“ in den Verzeichnissen zu stöbern und sich einen Überblick zu verschaffen, was dort alles verborgen ist.


*Die Unterverzeichnisse von „1. Listen, Pläne, Übersichten“*

Die grafischen Darstellungen finden Sie hier zu Beginn der Verzeichnisse als PDF, da dieses Dateiformat auf den meisten PCs zu öffnen ist. Nehmen Sie sich Zeit und schauen Sie sich die Grafiken, die Ihnen auffallen, genau an.

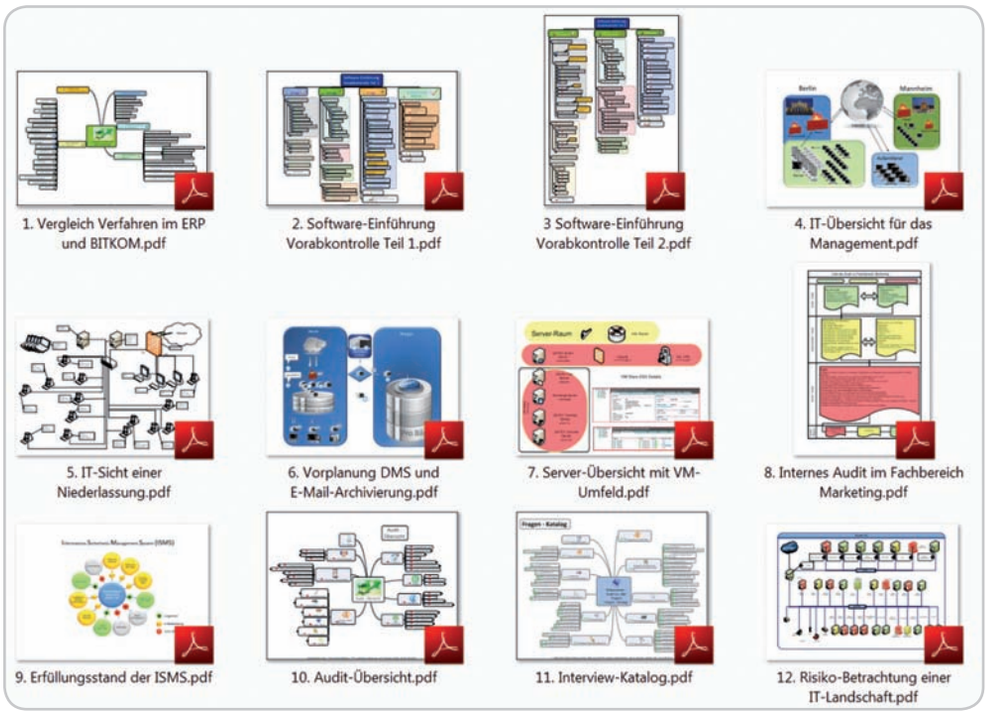



*Einige Beispiele für Listen, die auf der CD zu finden sind*




*Beispiele für Pläne*

Pläne haben einen hohen Wiedererkennungswert und sind sehr nützlich bei einer Kontrolle oder bei innerbetrieblichen Sicherheitsüberlegungen.




*Beispiele für Übersichten*

Was alles an Übersichten in den letzten Jahren entstanden ist, verblüfft mich oft selbst. Und die letzten Abbildungen sind nur ein kleiner Auszug aus dem, was Sie erwartet.

*Welche Software benötigen Sie?*

Wer diese Dateien an seine Wünsche anpassen möchte, benötigt auf seinem PC jedoch die Programme MS Power Point, MS Visio und MindManager.

Für MS Visio ist es mir nicht gelungen, ein alternatives Softwareprodukt zu finden. Auf dem Markt der Mindmap-Software dagegen hat sich in den letzten Jahren viel getan. Produkte wie „Webspiration“, „SpicyNodes“, „Mind42“, „LucidChart“, „gliffy“, „Creately“, „Bubbl.us“, „Xmind“, „mindmeister“, „spinscape“ und „Google Drawings“ können teilweise kostenfrei erworben werden, sind jedoch in den seltensten Fällen zueinander kompatibel.

Um alle Mindmaps in diesem Buch und in Ihrer künftigen Datenschutz-Dokumentation nutzen zu können, empfehle ich Ihnen, sich mit der Testversion des MindManager über die Möglichkeiten einer Mind-Software zu informieren und erst danach nach Alternativen zu suchen.

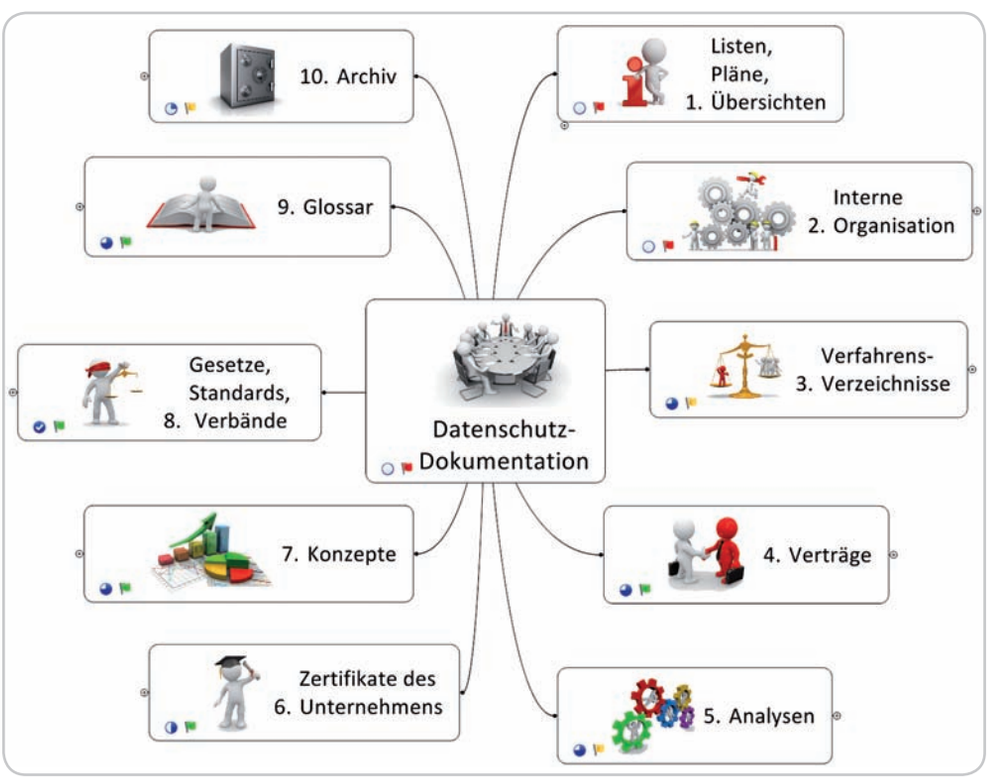
Tauchen Sie ein in eine Datenschutz-Welt aus Listen, Plänen und Übersichten, und behalten Sie den Überblick!

# III Vom Chaos zur klaren Datenschutz-Dokumentation

## III.1 Grundlagen der Datenschutz-Dokumentation

Das Bundesdatenschutzgesetz (BDSG) beinhaltet so viele Aufgaben eines Datenschutzbeauftragten, dass es auf den ersten Blick schwierig erscheint, alles zu beherrschen. Zulässigkeiten, Einwilligungen, Übermittlungen, Ausnahmen, Meldepflicht, Schulung der Mitarbeiter, Datengeheimnis, Rechte Betroffener, Speichermedien, Schadensersatz oder technische und organisatorische Maßnahmen sind nur eine Auswahl.

Wie soll ich meine Arbeit organisieren, wie soll ich meine Dokumentation aufbauen und pflegen? Eine Datenschutz-Dokumentation soll meine Arbeiten unterstützen und auch für andere Personen übersichtlich sein.




*Struktur der Datenschutz-Dokumentation*

*Grundidee der Dokumentation*

Die Grundidee dieser Datenschutz-Dokumentation ist:

- die Vielzahl an Dokumenten im Alltag eines Datenschutzbeauftragten zu beherrschen
- neue Aufgabenstellungen, Probleme oder Gesetzesänderungen in die Datenschutz-Dokumentation integrieren zu können, ohne die gesamte Struktur zu ändern
- eine umfassende Übersicht zu besitzen, von der aus sich jedes Dokument der Datenschutz-Dokumentation aufrufen lässt und in der der Stand der Arbeiten festgehalten werden kann

*Viele DSBs, viele Varianten*

Wenn es in Gesprächen unter Datenschützern um eine Datenschutz-Dokumentation geht, erfährt man so viele Lösungsvarianten, wie Gesprächsteilnehmer beteiligt sind. Von der Notlösung bis zum ausgefeilten Ablagesystem, vom einfachen Verfahrensverzeichnis-Formular bis zur gemeinschaftlichen Intranet-Bearbeitung hat jede Variante ihre Berechtigung.

Bei der Beantwortung folgender Fragen gehen die Meinungen auseinander:

- Was gehört alles in eine Datenschutz-Dokumentation?
- Für wen ist diese Dokumentation bestimmt?
- In welchem Zyklus soll eine Aktualisierung erfolgen?
- Wer entscheidet, welche Ausarbeitungen oder Vorgehensweisen eines Datenschutzbeauftragten verhältnismäßig sind?

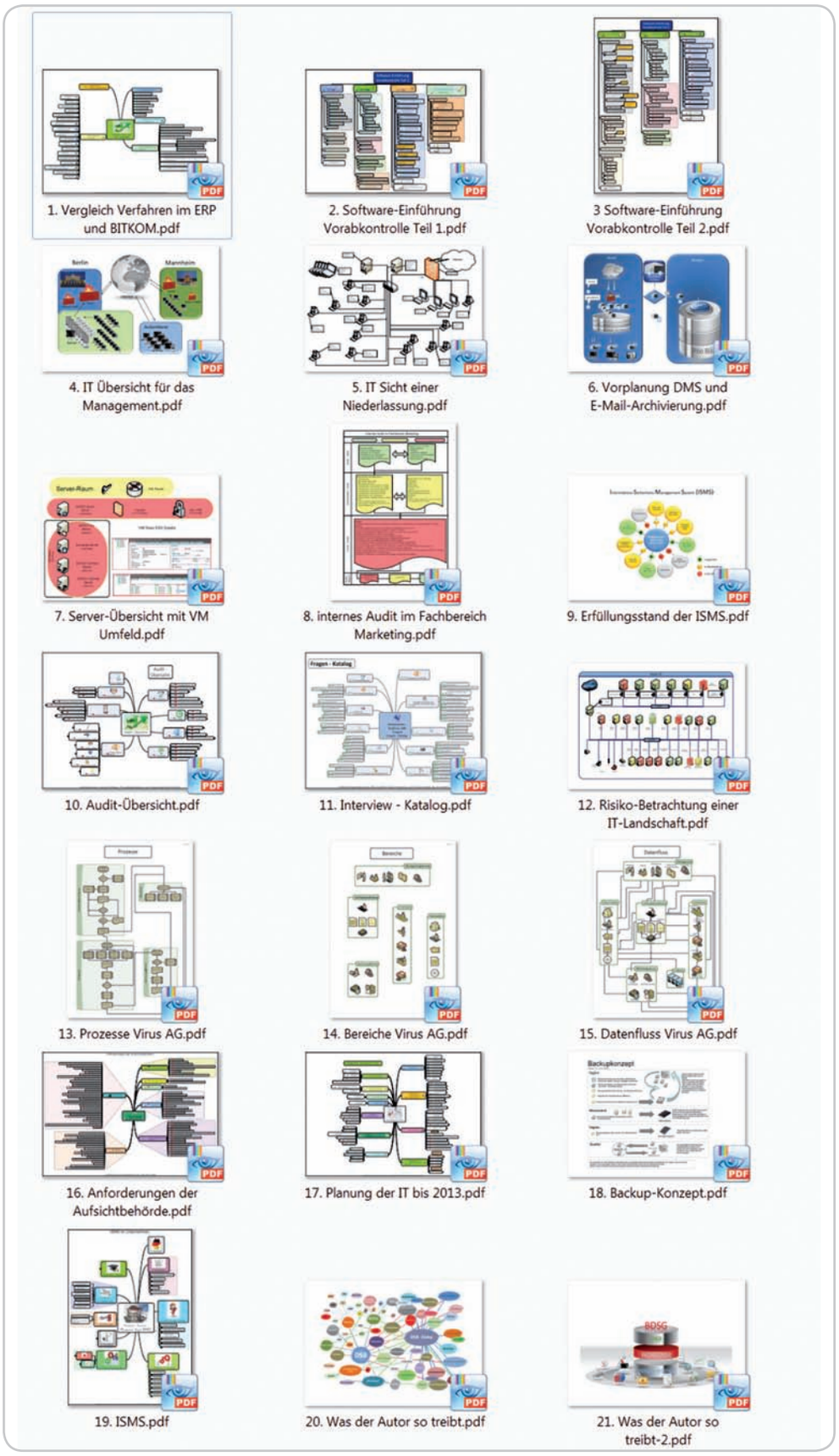
*Sie haben die Wahl!*

Ich werde für Sie meine Datenschutz-Dokumentation in ihre Einzelteile zerlegen. Sie suchen sich die Sahnestückchen heraus und stellen Ihre eigene Datenschutz-Dokumentation zusammen. Das Ergebnis Ihrer Mühen ist Ihr persönlicher Datenschutz-Ordner im Papier- und im Dateiformat.

*Auf einen Blick*

**Was erwartet Sie in diesem Kapitel?**

- Ich erläutere Ihnen, wie Sie diese Datenschutz-Dokumentation als Dateistruktur, als grafische Arbeitsplattform und als Ordner in Papierform für Ihre Zwecke nutzen können.
- Sie erhalten einen Fundus von Checklisten, Grafiken, Plänen und Organigrammen, aus denen Sie die für Sie interessanten auswählen. Alle Dateien stehen für Sie in bearbeitbarem Format zur Verfügung.
- Nachdem Sie sich einen umfassenden Eindruck verschafft haben und wissen, welche Ausarbeitungen für Sie passend sind, bauen wir Ihre eigene Datenschutz-Dokumentation zusammen.




*Beispieldokumente aus der Datenschutz-Dokumentation*

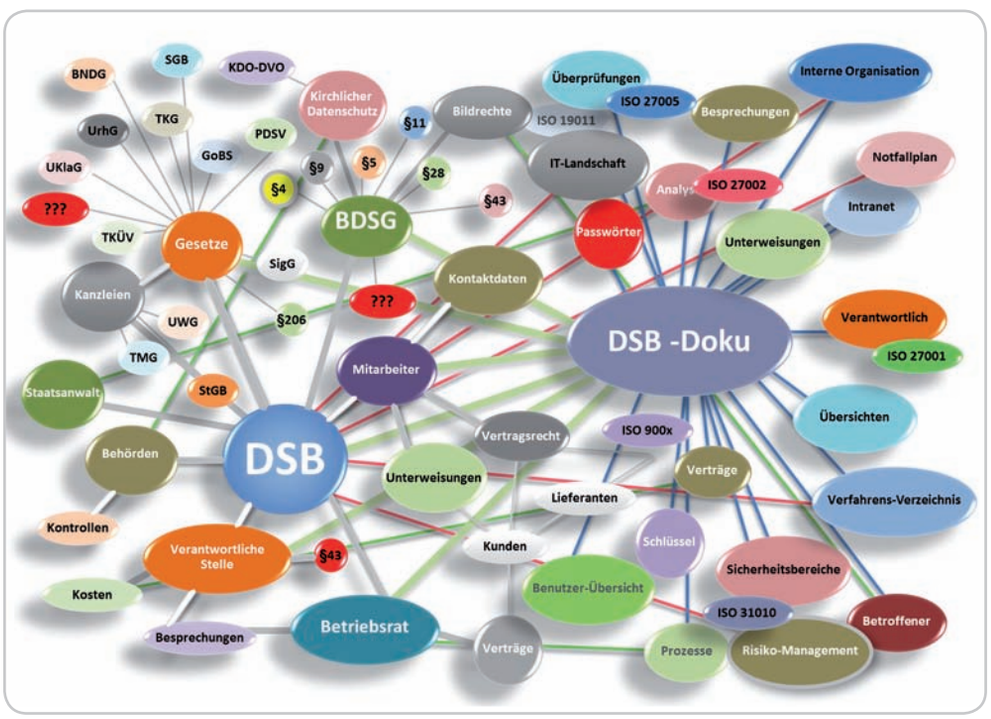

*Einer meiner Datenschutz-Ordner*

Bei der Auswahl Ihrer Favoriten aus dem Fundus von Beispielen und Mustern helfe ich Ihnen. Genau diese Favoriten werden dann im Kapitel „III.3. Ihre Datenschutz-Dokumentation“ Bestandteil Ihrer eigenen Datenschutz-Dokumentation und Ihres Datenschutz-Ordners.

## III.1.1 Wohin mit den vielen Dokumenten?

Für mich haben chaotische Aufgaben und Probleme eine große Anziehungskraft. Warum, kann ich nicht beantworten, aber jedes Mal entstand aus dem Chaos etwas völlig Neues.

Der Versuch, komplizierte Problemstellungen so zu vereinfachen, dass sie allgemein verständlich werden, stellt eine echte Herausforderung dar. Wohin mit Mitarbeiterlisten, Gebäudeübersichten, Organigrammen, Tätigkeitsberichten, Intranet-Auftritten, Vertragsarbeiten, Standards, Analysen, Prozessen und Verträgen? Sie werden diese Aufzählung sicher um einige Punkte erweitern können.




*Ordnung oder Chaos?*

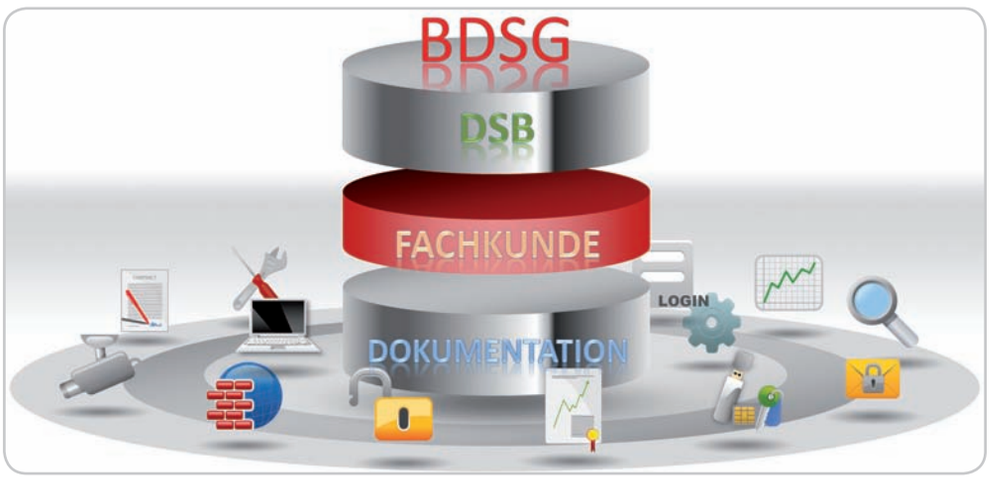
So oder so ähnlich könnte es auch in Ihrem Kopf nach Ihrer Berufung zum Datenschutzbeauftragten oder nach einer Weiterbildung ausgesehen haben. Die Neueinsteiger unter Ihnen werden sich fragen, wie sie die komplexen Themenbereiche bewältigen sollen. Die alten Hasen werden anmerken, dass da ja noch die TOMs (technisch-organisatorische Maßnahmen) sowie Details der internen Verfahrensübersichten fehlen.

Weiterhin wird Ihre Arbeit als Datenschutzbeauftragter noch beeinflusst von

- der jeweiligen Branche,
- Ihren speziellen Fähigkeiten,
- unerwarteten Sicherheitsvorfällen,
- Gesetzesänderungen,
- Auftraggebern, Kunden und Lieferanten,
- der Entwicklung Ihres Unternehmens auf dem Markt,
- der Präsenz des Datenschutzes in den Medien
- und, und, und …

Wie soll man Datenschutz beherrschen und im Unternehmen oder bei Kunden allgemein verständlich vermitteln?

Organisieren wir das Chaos und erzeugen Bilder, die uns an etwas aus dem Datenschutz erinnern sowie unseren Arbeitsbereichen und Problemstellungen Struktur verleihen:




*Die Welt des Datenschutzbeauftragten*

Zu jedem Icon in dieser Grafik fällt Ihnen eine Ihrer Aufgaben ein. Zu jedem Icon die Vorgänge und Problemstellungen zu dokumentieren und wiederzufinden, wird etwas schwieriger. Die Übersicht über den Stand Ihrer Arbeit, die Entwicklung Ihres Unternehmens, die Weiterentwicklung der IT und die Aufrechterhaltung Ihrer Fachkunde nicht zu verlieren, stellt sich als echte Herausforderung heraus.

An dieser Stelle möchte ich Sie mit dieser Datenschutz-Dokumentation unterstützen. Was bezwecke ich also mit dieser Datenschutz-Dokumentation?

1. Die Datenschutz-Behörden oder externe Prüfer sollen sich schnell in der Datenschutz-Dokumentation zurechtfinden und die gute Arbeit des Datenschutzbeauftragten erkennen.
2. Die verantwortliche Stelle soll Vorteile für das Management erkennen und die Arbeiten des Datenschutzbeauftragten schätzen.
3. Ihre Arbeit als Datenschutzbeauftragter soll einfacher und übersichtlicher werden und vielleicht sogar ein wenig Spaß machen.

Daraus abgeleitet teilt sich die Datenschutz-Dokumentation für mich in drei Bereiche ein:


*Die drei Bereiche der Datenschutz-Dokumentation: Dateiablage, Mindmap und Ordner*

1. die Dateiablage (ablegen, verschlüsseln, transportieren, sichern)
2. die grafische Arbeitsplattform (verständlich, transparent, kompetent)
3. der Ordner in Papier (nachschlagen, kontrollieren, präsentieren)

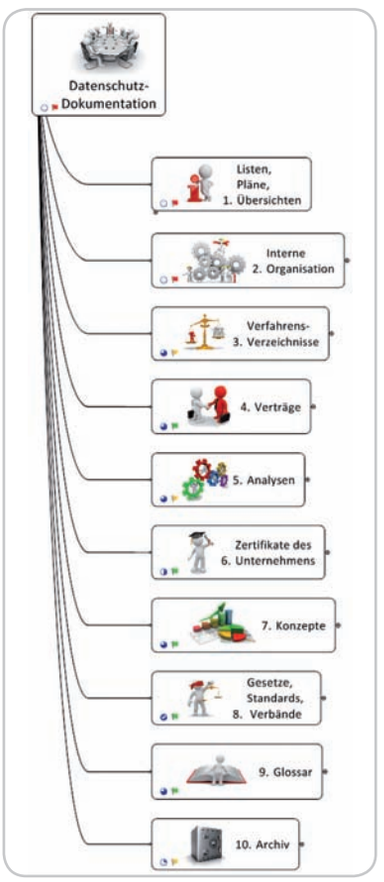
*Identischer Aufbau*

Die Einteilung der Dateiablage, der grafischen Abbildung in einer Mindmap-Darstellung und des Ordners in Papier stimmen überein.


Die Dateiablage, deren Inhalte Sie an Ihr Unternehmen anpassen können, besteht aus Checklisten, Vertragsmustern, Organigrammen, Prozessabläufen und Grafiken. Sie befindet sich auf der CD. Alle Dokumente, Grafiken und Pläne liegen in bearbeitbaren Dateiformaten vor.

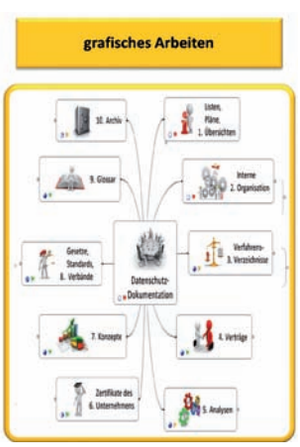
Die Dokumente über den Dateiexplorer zu nutzen, stellt einen bequemen Weg dar. Bei einer großen Anzahl an Dokumenten fällt es mir jedoch schwer, mit diesem Windows-Werkzeug den Gesamtüberblick zu behalten. Daher arbeite ich gern mit Mindmaps, die sich identisch aufbauen lassen:


*Dateiablage im Explorer*



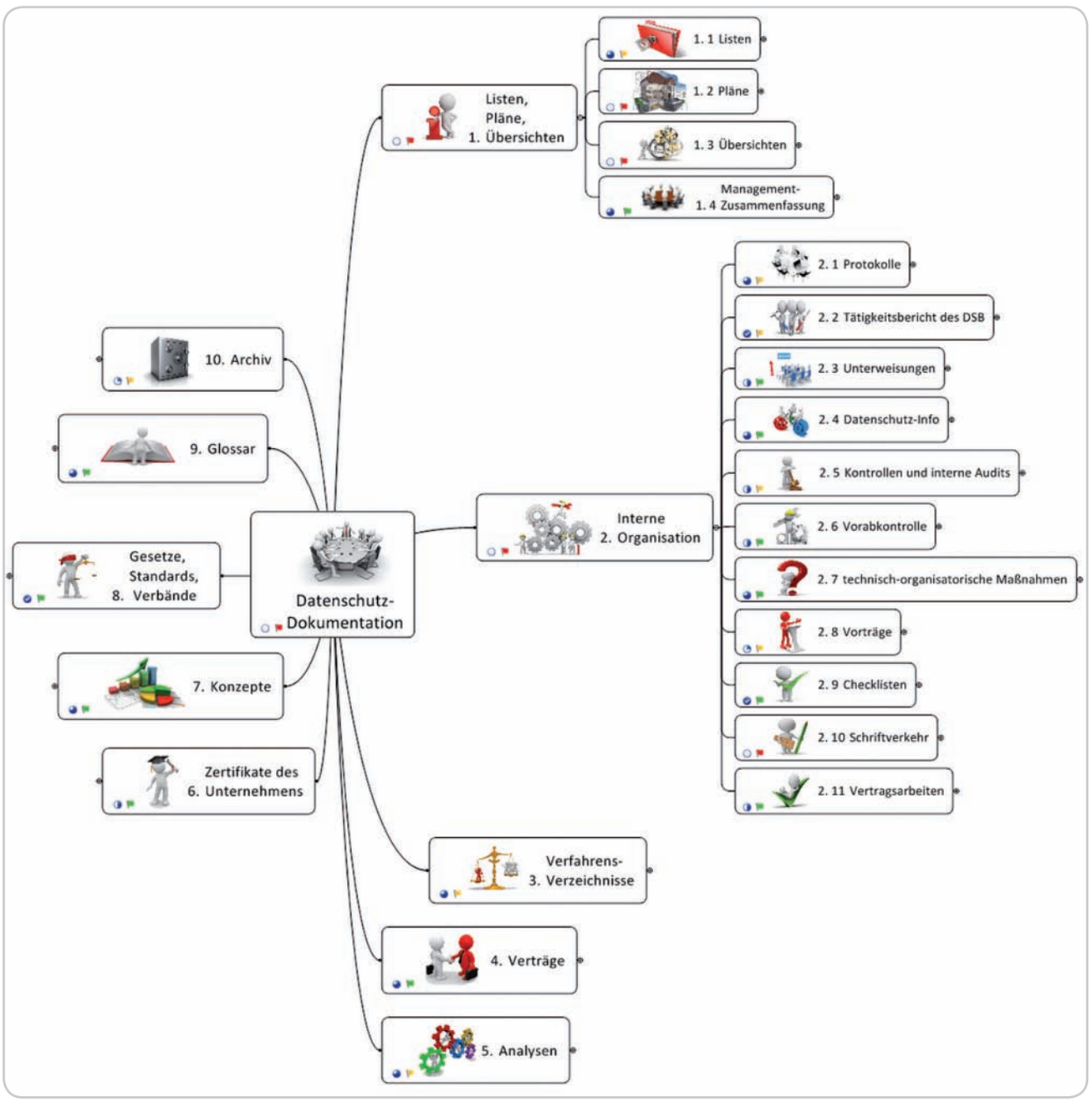

*Darstellung als Mindmap im MindManager*

Jedes Unterverzeichnis auf der Dateiebene stimmt mit dem in der Mindmap-Darstellung überein. Was wir Verzeichnis oder Unterverzeichnis in einer Dateistruktur nennen, wird in einer Mindmap (MindManager-Datei) als Zweig oder Unterzweig bezeichnet. Im weiteren Text ist diese Unterscheidung für Sie wichtig: Spreche ich von einem Zweig, befinden wir uns immer in einer Mindmap des MindManager.



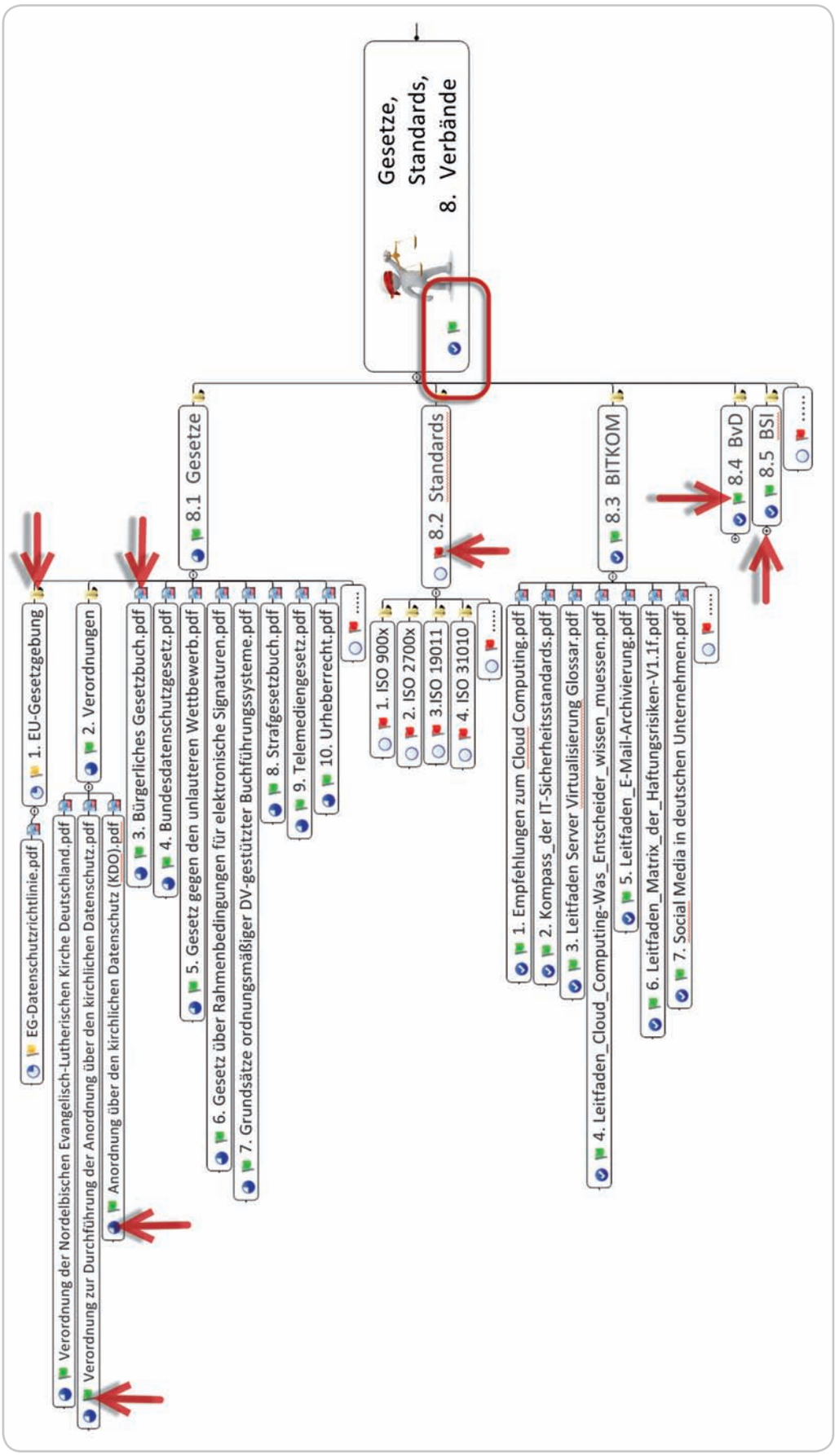

Die grafische Ausgestaltung in einer Mindmap stellt eine Besonderheit dar. Bereits nach kurzer Eingewöhnung werden Sie erkennen, wie zeitsparend die Nutzung des Mindmap-Werkzeugs bei Ihrer Arbeit als Datenschutzbeauftragter sein kann. Vorgefertigte Muster erleichtern Ihnen den Einstieg – natürlich alles praxiserprobt und auf der beiliegenden CD.

Größer und mit aufgeklapptem Unterzweig sieht das Ganze so aus:




*Datenschutz-Dokumentation mit offener interner Organisation; mit Flaggen und Erfüllungsgrad*

Mittels einfacher Fähnchen (Flaggen) sehe ich auf einen Blick, an welcher Stelle meiner Datenschutz-Dokumentation ich noch etwas arbeiten muss (rot und gelb) und an welcher Stelle alles erledigt ist (grün).




*Beispiel einer umfangreichen Dokumentenübersicht im Unterzweig „Gesetze, Standards, Verbände" mit Flaggenkennzeichnung in den Ampelfarben*

## III.1.2 Der Umfang der Datenschutz-Dokumentation

Die Diskussion über den Umfang der Datenschutz-Dokumentation ist unmittelbar mit der Frage nach der Verhältnismäßigkeit verbunden.

*Unternehmensgröße ist nicht entscheidend*

Leider geben die Größe Ihres Unternehmens und die Anzahl Ihrer Mitarbeiter nur wenige Rückschlüsse auf den Umfang Ihrer Datenschutz-Dokumentation. Ein Großhandelszulieferer für Heizungstechnik mit 350 Mitarbeitern kann eine kleinere Dokumentation benötigen als ein Softwareunternehmen mit 50 Mitarbeitern und 25.000 Direktkunden.

*Wichtige Faktoren*

Ich bin der Meinung, dass sich vor allem folgende Aspekte auf den Umfang einer Datenschutz-Dokumentation auswirken:

- Wie viele Niederlassungen, Gebäude, Etagen und Home-Arbeitsplätze haben Sie zu betreuen?
- Wie viele Mitarbeiter haben mit automatisierter Verarbeitung von personenbezogenen Daten zu tun? Zentrale Frage: Wer besitzt die Möglichkeit, mittels Internet oder E-Mail eine Kommunikation von oder nach außerhalb Ihres Unternehmens aufzubauen?
- Wer führt die Datenschutzunterweisungen durch?
- Welchen Stellenwert haben Qualitäts-, Risiko-, Notfall- und IT-Management im Unternehmen?
- Wie umfangreich sind die Vertragsarbeiten, z.B. Vertraulichkeit oder § 11 BDSG (Verarbeitung im Auftrag)?
- In wie vielen Verfahren werden personenbezogene Daten verarbeitet?

Die Beantwortung dieser Fragen ist in keinem Unternehmen meines Arbeitsumfelds, selbst bei gleicher Branche, gleich.

*Was ist verhältnismäßig?*

Jetzt ist nur noch zu klären, wie tief wir in die einzelnen Themen eintauchen (Verhältnismäßigkeit). Leider werden Sie auch hier keine klaren Antworten erhalten. Diese Beispiele vermitteln Ihnen meine Vorstellungen dazu:

- Die DIN eines Sicherheitsschlosses zu ermitteln, ist unverhältnismäßig. Ob im Erdgeschoss Sicherheitsglas eingebaut ist, ist verhältnismäßig.
- Die BIOS-Version und technische Details eines Servers zu ermitteln, ist unverhältnismäßig. Festzustellen, welche Software auf ihm installiert ist, ist verhältnismäßig.
- Wöchentlich das Verfahrensverzeichnis zu überarbeiten, ist unverhältnismäßig. Eine halbjährliche oder jährliche Aktualisierung ist verhältnismäßig.

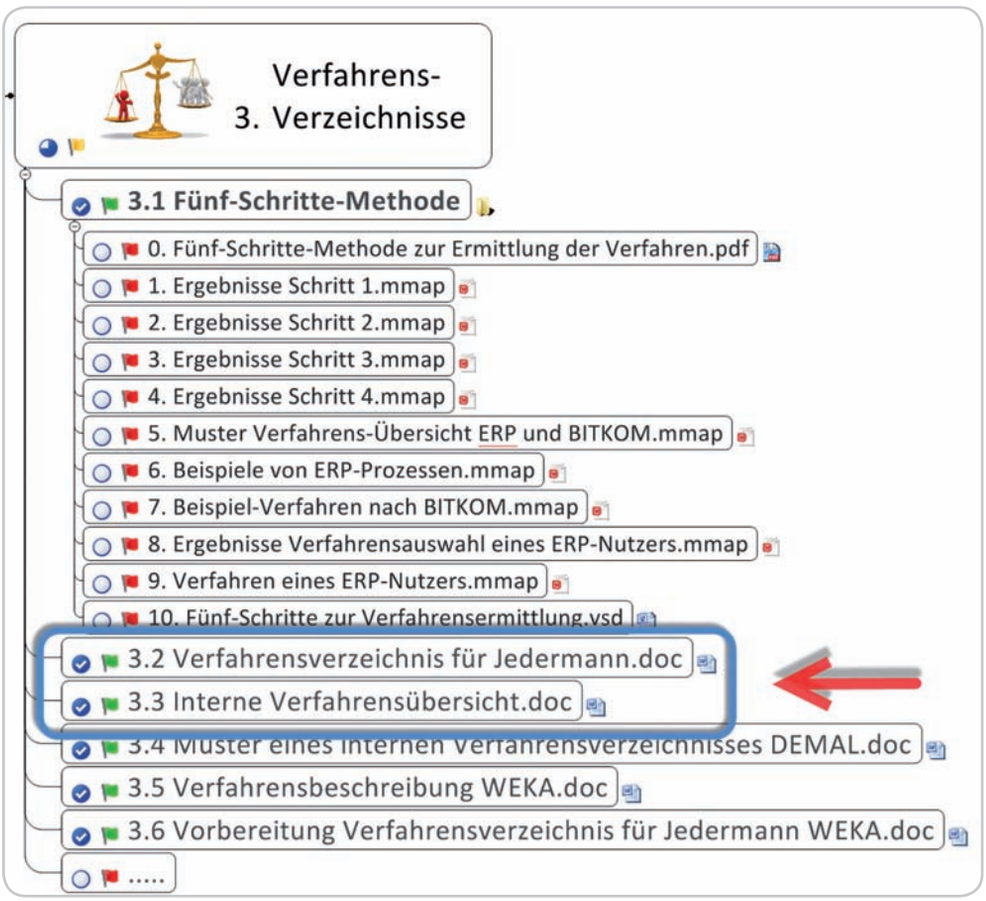
Umfang und Verhältnismäßigkeit Ihrer Datenschutz-Dokumentation sollten Sie immer im Blick behalten. Ich habe die vorliegende Dokumentation mit so vielen Vorlagen, Beispielen und Mustern bestückt, dass der Gesamtumfang sicher „unverhältnismäßig“ ist. Sorgen Sie dafür, dass ein ausgewogenes Verhältnis zu Ihrem Unternehmen und Ihren Vorstellungen entsteht.

*Tipp*

Ich empfehle, auch den zeitlichen Aufwand mit dem Nutzen für Ihr Unternehmen und für den Datenschutz in Relation zu setzen.

## III.2.3.1 Verfahrens-Verzeichnisse

*Prozesse oder Verfahren?*




*Verfahrensverzeichnisse*

Wenn ich ein Verfahrensverzeichnis bearbeite, erinnere ich mich oft an meine ersten Versuche, herauszubekommen, was alles ein Verfahren ist. Die Geschäftsleitung hat damals nicht verstanden, was ich unter Verfahren verstehe, und ich war auch nicht in der Lage, Verfahren gut zu verdeutlichen.

*Tipp*

> Der Grund für diese Situation ist aus meiner heutigen Sicht klar: Eine Geschäftsleitung denkt in Wertschöpfungsprozessen, Produktentwicklungsprozessen, Produkterstellungsprozessen, Unterstützungsprozessen, Kernprozessen etc., nicht in Verfahren.

Bei meiner Suche nach einer Lösung bin ich auf das Wort „Verfahren" im Qualitätsmanagement gestoßen, und zwar bei Verfahrensanweisungen (VAs). Diese Zusammenhänge verstand jedoch nur der Qualitätsmanager (QM), die Geschäftsleitung nicht.

*Mit Prozessen allein kann ein DSB wenig anfangen*

Nach § 4g Abs. 2 BDSG soll uns die verantwortliche Stelle, also die Spezialisten für Prozesse, eine Verfahrensübersicht übergeben. Leider ist mir das bisher noch nie passiert. Und ohne meine Erläuterung hat auch noch kein Geschäftsführer beantworten können, was ein Verfahren im datenschutzrechtlichen Sinn ist. Wenn ich nach einem Prozess gefragt hätte, wäre seine Antwort sicher anders ausgefallen.

Eine Übersicht der Verfahren, die ein Beauftragter für Datenschutz von seiner verantwortlichen Stelle erhält, ist also im besten Fall eine Zusammenstellung von Prozessen. Was ist dann aber ein Verfahren?

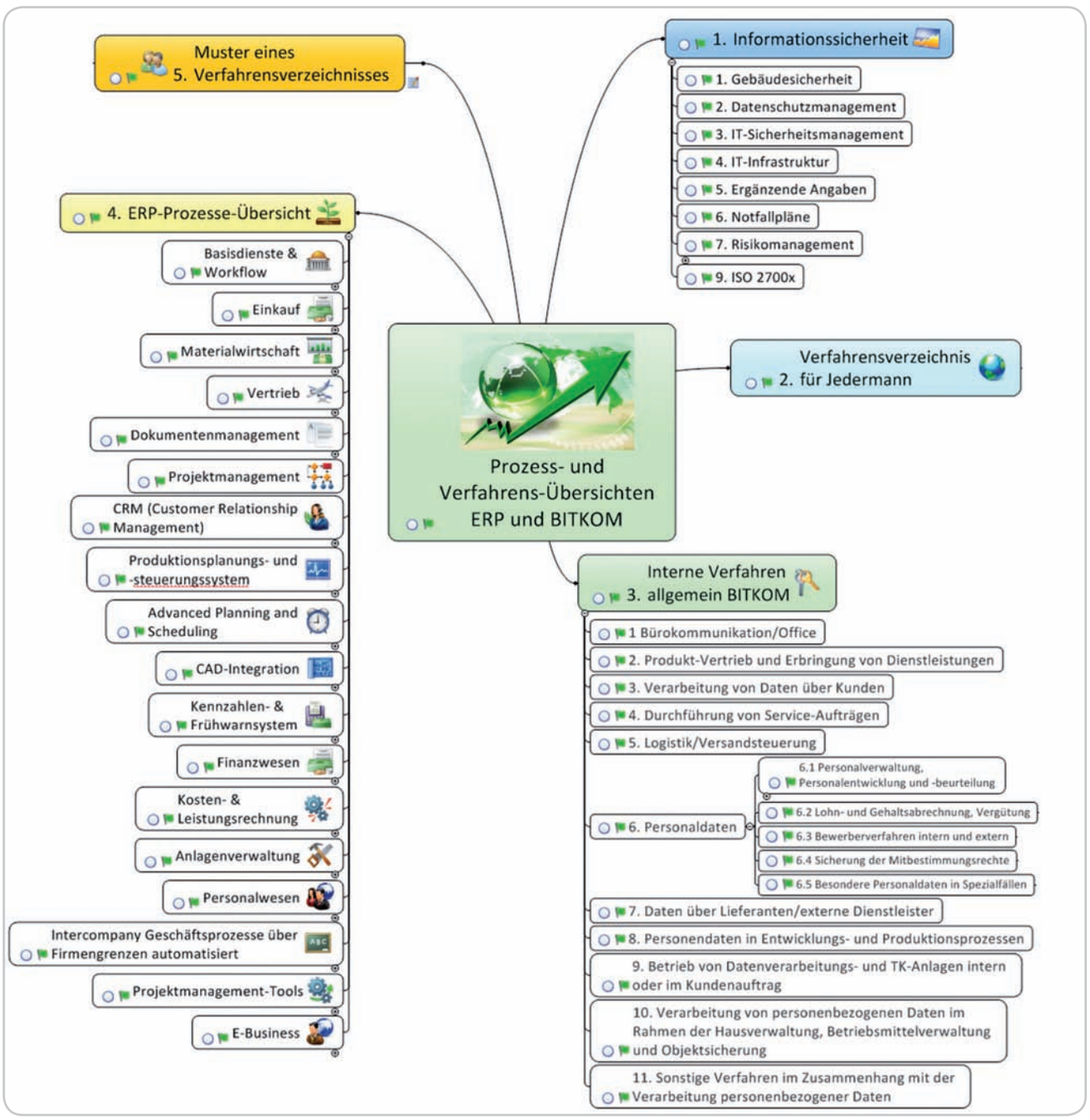
*Wie sind „Verfahren" definiert?*

Wenn es um die Definition des Begriffs „Verfahren" im Datenschutz geht, müssen wir den Artikel 18 der EG-Datenschutzrichtlinie heranziehen. Die Interpretation, dass ein Bündel von Verarbeitungen mit gleichem Zweck ein Verfahren darstellt, ist jedoch nicht glücklich gewählt. Wikipedia trifft es für mich besser: „Verfahren steht für einen geregelten, in Verfahrensschritte zerlegbaren, nachvollziehbaren und wiederholbaren Ablauf". Auch das lässt immer noch einen großen Spielraum zu, ist aber schon etwas, mit dem man als DSB arbeiten kann.

Ich habe noch keinen Datenschutzbeauftragten kennengelernt, der das Erstellen einer internen Verfahrensübersicht als einfach bezeichnet hat. Selbst das Vergleichen unterschiedlicher Verfahrensübersichten lässt keine Verallgemeinerung zu, die für jeden Datenschutzbeauftragten nutzbar wäre. Dass die Herangehensweise in jedem Hilfsmittel oder Softwaretool anders ist, erschwert die Situation zusätzlich. Ich stelle Ihnen daher einmal meine Methode vor, die in verschiedenen Unternehmen von Koordinatoren oder Datenschutzbeauftragten genutzt wird.

*In fünf Schritten zu meinen Verfahren*

Bevor Sie beginnen, eine interne Verfahrensübersicht zu erstellen, müssen Sie ergründen, welche Verfahren des Unternehmens personenbezogene Daten enthalten. Bei den ersten Besprechungen steige ich mit der Übersicht einer Verfahrensübersicht ein, um einen groben Überblick des Unternehmens zu erhalten.




*Mindmap „Muster Verfahrensübersicht ERP und BITKOM“*

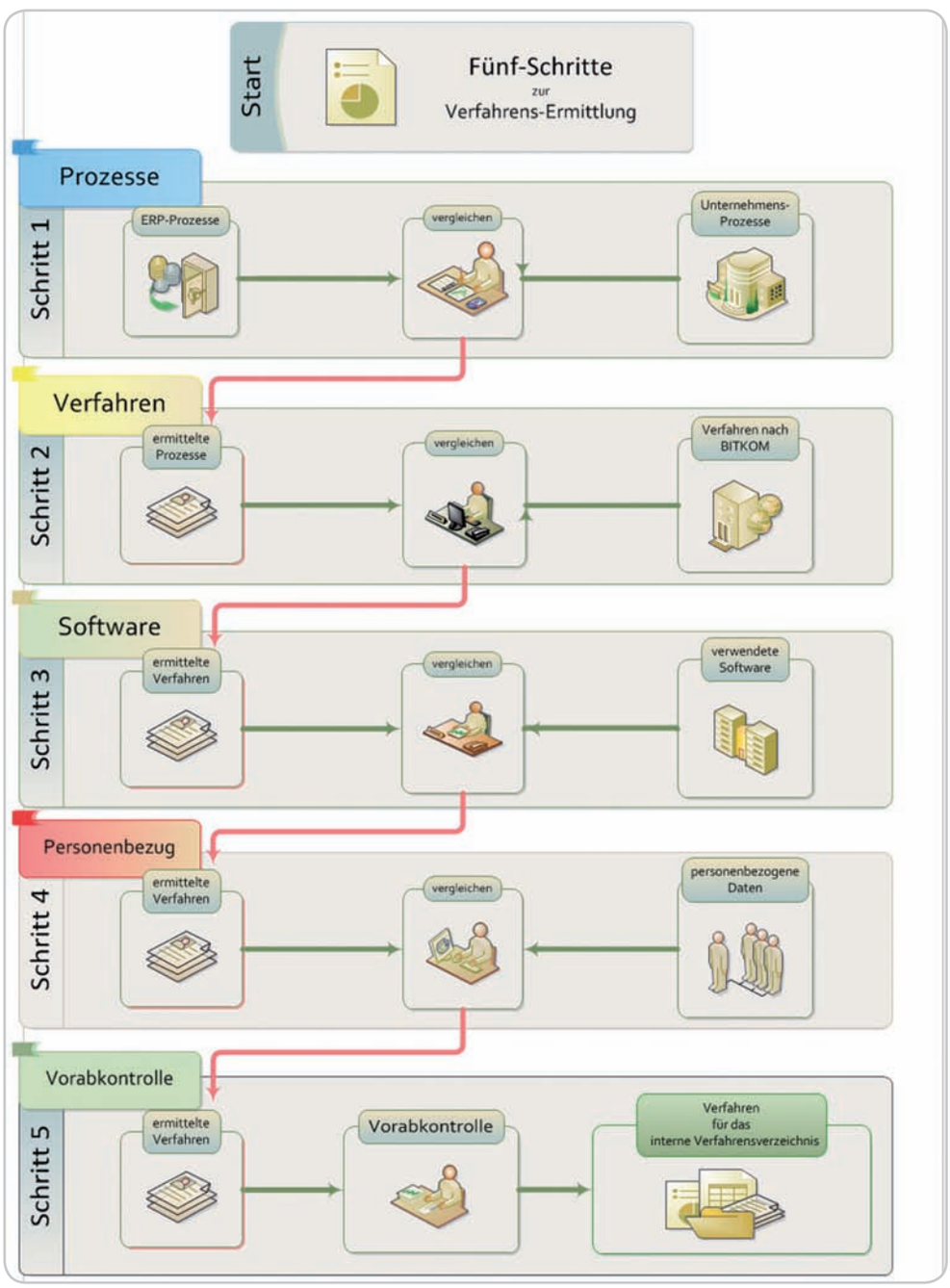
Seit Jahren betreue ich einen Softwareentwickler für ERP-Anwendungen. ERP steht für Enterprise Resource Planning, also Unternehmensressourcenplanung. Der Begriff bezeichnet „die unternehmerische Aufgabe, die in einem Unternehmen vorhandenen Ressourcen (Kapital, Betriebsmittel oder Personal) möglichst effizient für den betrieblichen Ablauf einzusetzen und somit die Steuerung von Geschäftsprozessen zu optimieren“ (Quelle: Wikipedia). Bei meiner Arbeit als Datenschutzbeauftragter ist mir aufgefallen, dass vor dem Programmieren der einzelnen ERP-Module jeder innerbetriebliche Ablauf analysiert wird und die Grundlage einer ERP-Software ist.

*ERP nimmt Datenflüsse unter die Lupe*

Das Merkwürdige für mich war, dass man genau das tat, was jeder Datenschutzbeauftragte tut: Der Datenfluss im Unternehmen wird unter die Lupe genommen. Der einzige Unterschied besteht im verfolgten Ziel. Während im ERP nach Optimierungen für das Unterneh-

men gesucht wird, interessiert sich der Datenschutzbeauftragte für den Datenfluss von personenbezogenen Daten. Auch wenn in dieser ERP-Optimierungswelt andere Begriffe benutzt werden, passten viele der ermittelten Prozessabläufe zu meinen ermittelten Verfahren. Diese Erkenntnis war der erste Schritt zur Entwicklung der Fünf-Schritte-Methode.

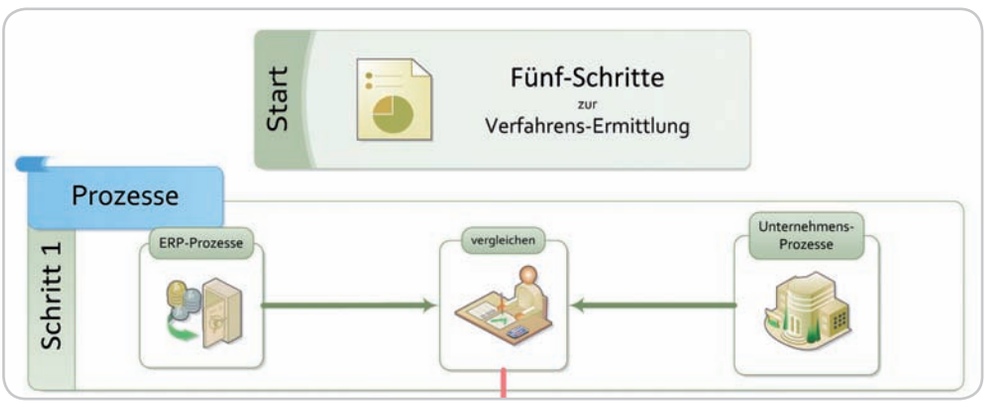
Wenn ich die Aufgabe erhalte, eine neue interne Verfahrensübersicht zu erstellen, ermittle ich die Datenschutzverfahren in fünf Schritten:




*Fünf Schritte zur Ermittlung der Verfahren*

### Die Fünf-Schritt-Methode im Einzelnen

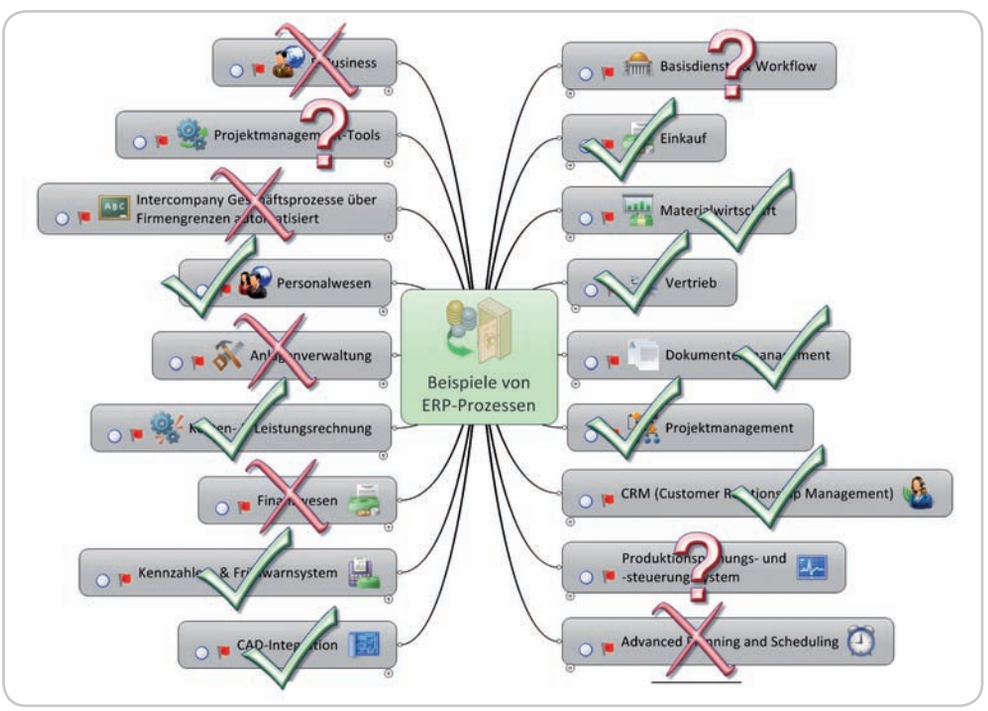
*Schritt 1: Prozesse*




*Schritt 1: Prozesse*

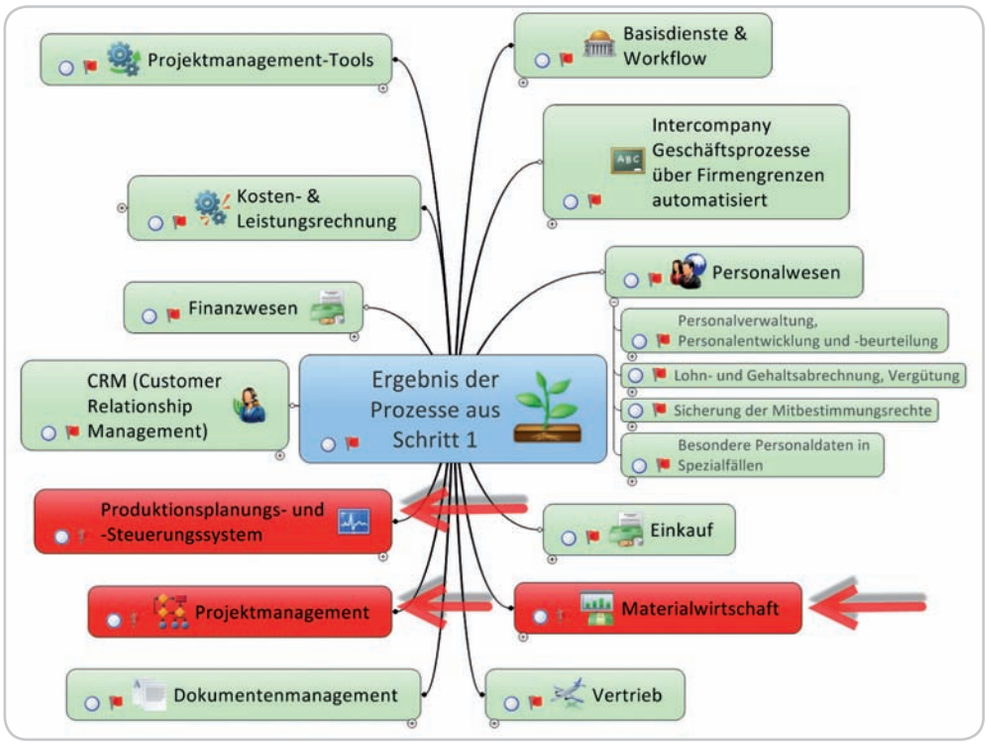
*Schritt 1: Vergleich der Prozesse*

Ich vergleiche zunächst sämtliche Unternehmensprozesse mit meiner Beispielübersicht von ERP-Prozessen. Sie finden diese Prozesse im Zweig „3. Verfahrensverzeichnisse“\ „3.1 Fünf-Schritte-Methode“ in der Datei „Beispiele von ERP-Prozessen.mmap“.




*ERP-Prozesse eines realen Unternehmens*

In dieser Mindmap streiche ich alle Prozesse, die auf mein Unternehmen nicht zutreffen, und kläre eventuelle Fragen zu den Prozessen mit dem Management im Unternehmen. Am Ende dieses Schritts könnte Ihr Ergebnis an Prozessen so aussehen:

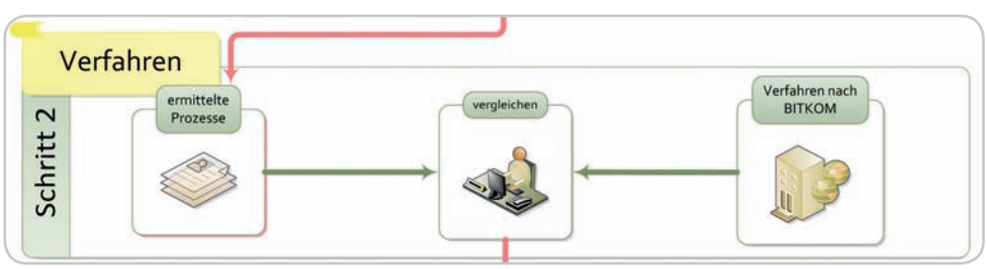



*Das mögliche Ergebnis eines Vergleichs zwischen ERP-Prozessen und Ihrem Unternehmen*

Die rot markieren Prozesse überprüfe ich nochmals, da mich die Antworten des Managements nicht zufriedenstellen.

*Schritt 2: Verfahren*

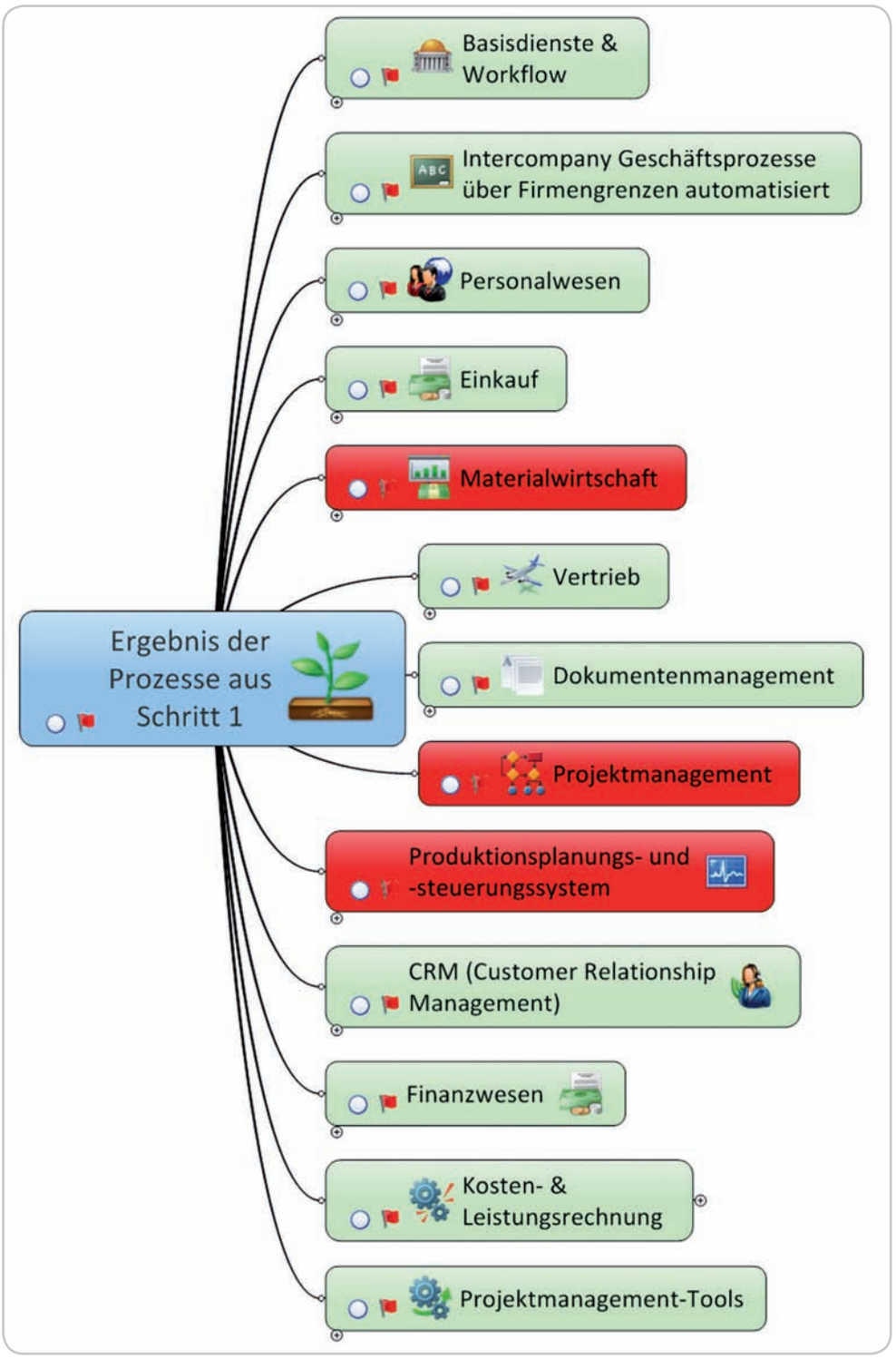
*Schritt 2: Vergleich mit BITKOM-Verfahren*



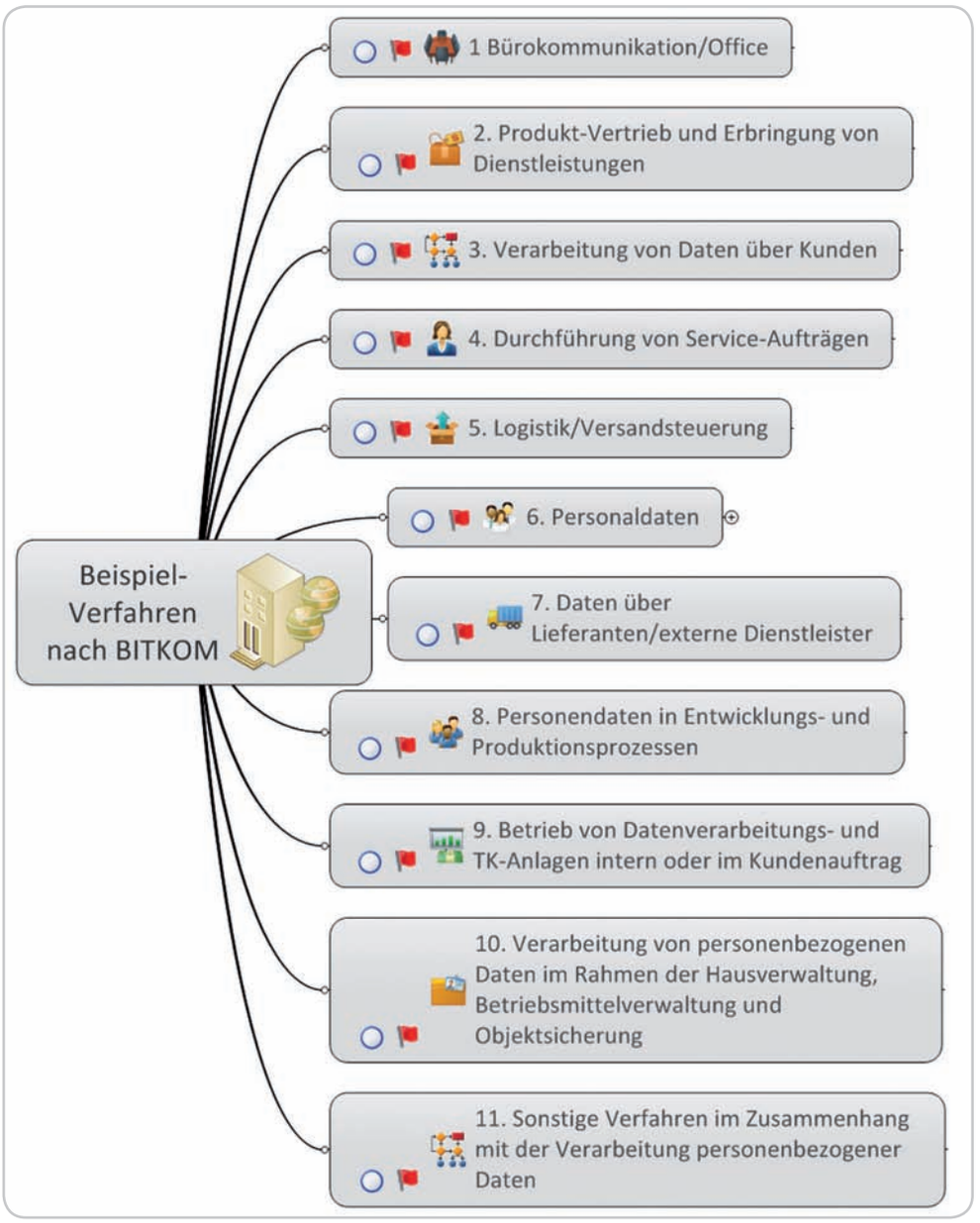

*Schritt 2: Verfahren*

Die ermittelten Prozesse aus Schritt 1 untersuche ich auf Gemeinsamkeiten mit den Datenschutzverfahren des BITKOM und nehme weitere Ergänzungen oder Streichungen von Prozessen oder Verfahren vor. Die BITKOM-Verfahren finden Sie in der Mindmap „Beispiel-Verfahren nach BITKOM.mmap".

Um Missverständnisse zu vermeiden, lasse ich mir in den meisten Fällen von den Verantwortlichen im Unternehmen erläutern, was sie unter den Prozessen verstehen. Dieser Schritt ist wichtig, da oft unterschiedliche Vorstellungen im Unternehmen bestehen, was genau der jeweilige Prozess bewirkt.

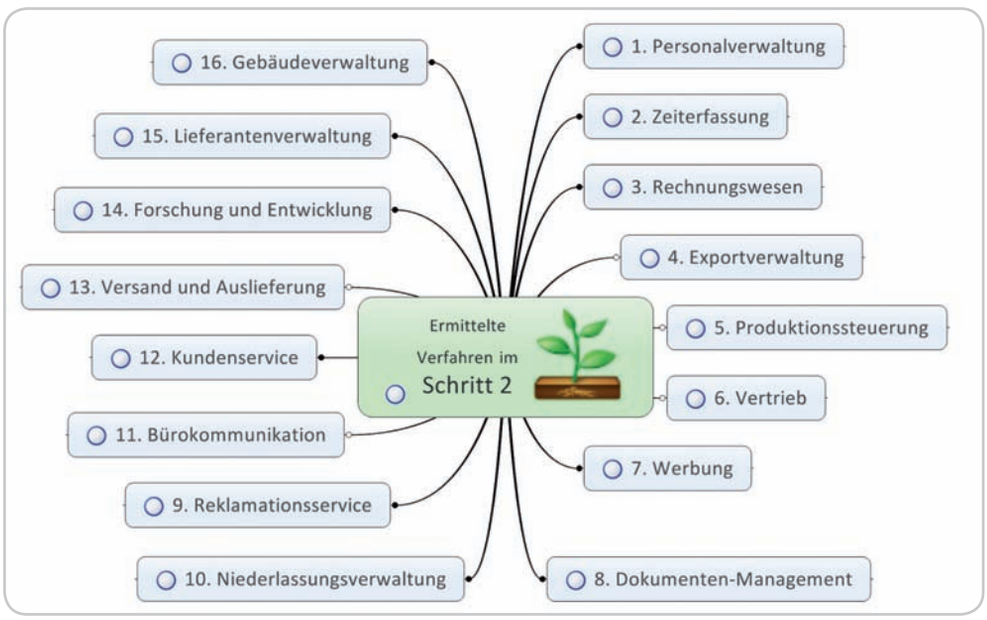



*Prozesse nach dem Vergleich mit dem eigenen Unternehmen*




*Verfahren aus der Sicht des BITKOM*

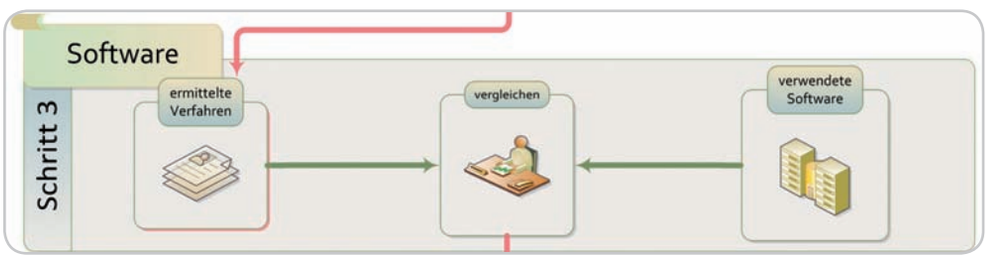
Beim Vergleich finden Sie Übereinstimmungen in Prozessen und Verfahren. Das Ergebnis betrachten wir als Verfahren unter Datenschutzgesichtspunkten und können so ganz auf Verfahren umsteigen. So entsteht eine erste Übersicht über die vorhandenen Verfahren im Unternehmen:




*Ermittelte Verfahren (Ergebnisse Schritt 2.mmap)*

Ob es sich um Datenschutzverfahren handelt, interessiert in dieser Phase noch nicht!

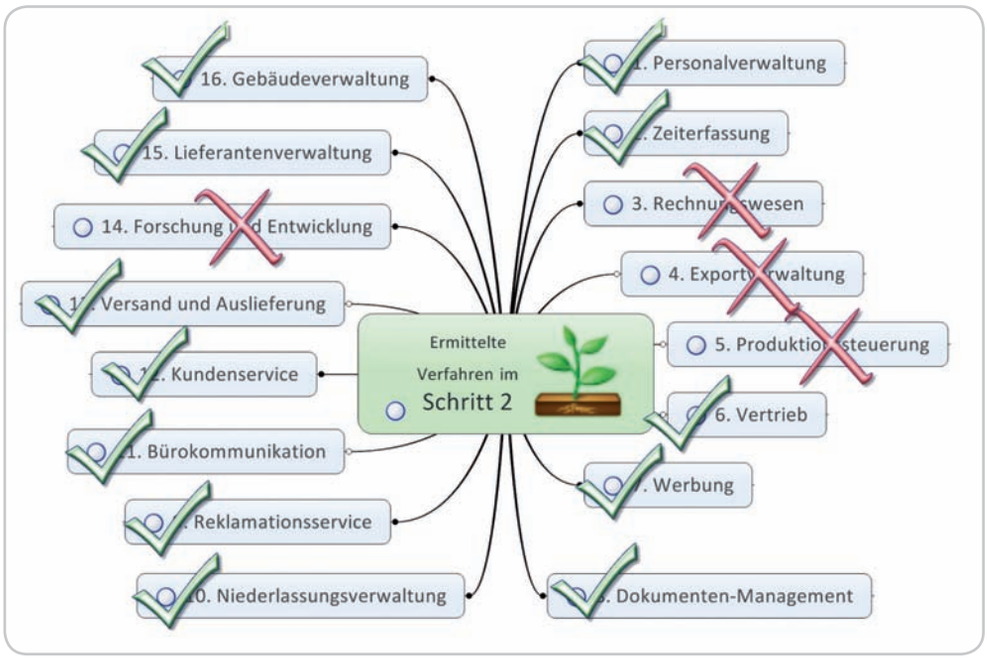
*Schritt 3: Software*




*Schritt 3*

*Schritt 3: Software*

Jetzt verfüge ich über die Verfahren des Unternehmens, die ich mit der eingesetzten Software abgleiche. Im Schritt 3 stelle ich mir also die Frage: Mit welcher Software wird welches Verfahren bearbeitet? Hier greife ich auf die „Software Zusammenfassung.docx“ aus dem Zweig „Listen“ zurück.




*In welchem Verfahren könnten personenbezogene Daten verarbeitet werden?*

*Eines oder mehrere Verfahren?*

Oft erkennen Sie aus dem Zweck und den Berechtigungsstrukturen weitere Verfahren oder können andere streichen. Eine Software pauschal als ein Verfahren zu betrachten, kann oft hilfreich sein. Ich rate jedoch davon ab, da es vorkommen kann, dass eine Software verschiedene Verfahren verarbeitet. Wenn der Zweck und die verantwortlichen Personen unterschiedlich sind, spricht das für mehrere Verfahren.

*Beispiel*

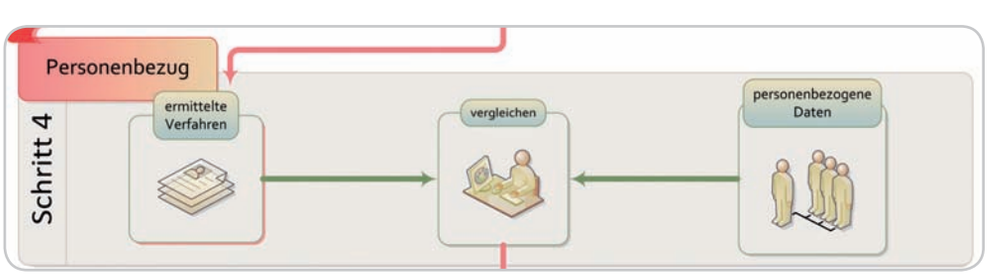
Ein Beispiel: Ein Softwareprodukt besteht aus den Modulen Stammdatenverwaltung, Mandantenverwaltung, Dienstpläne, Lohn und Gehalt, Zeiterfassung und Finanzbuchhaltung. Jetzt wäre es zu einfach, nur auf die Stammdaten zu verweisen, da dort personenbezogene Daten liegen. Es ist noch zu klären:

- wie die Daten in diesem Modul verarbeitet werden
- wer verantwortlich für die Verarbeitung ist
- welcher Personenkreis zu den Betroffenen zählt
- ob die Daten ins Ausland versendet werden

Sollten Sie auf so ein Problem stoßen, gehen Sie nicht sofort in die Detailprüfung, sondern warten Sie auf das Ergebnis des Schrittes 5.

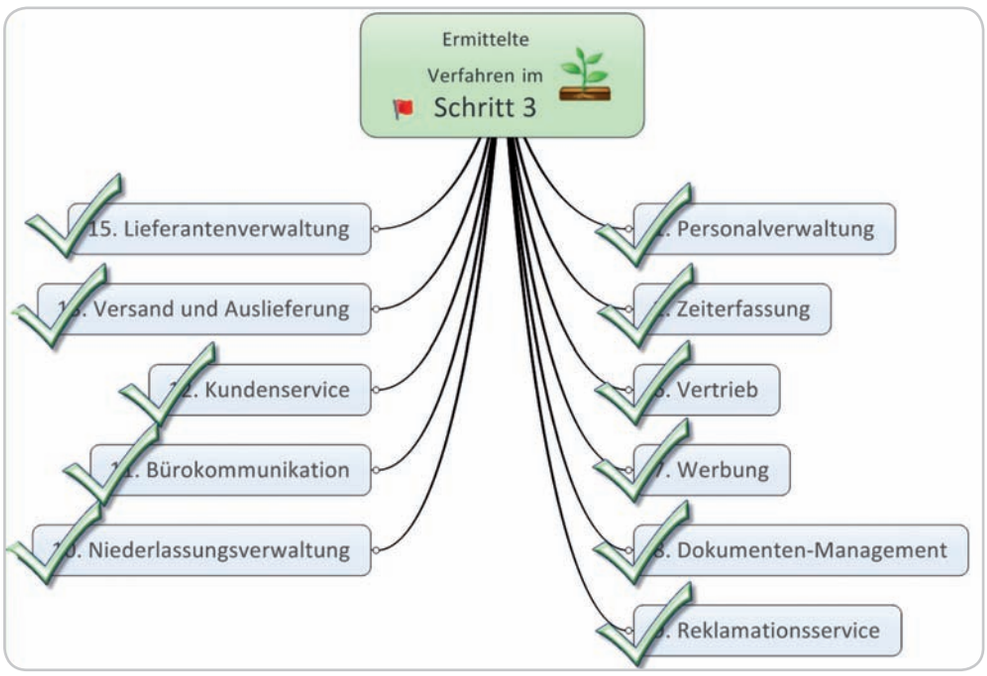
*Schritt 4: Personenbezug*

*Schritt 4: Datenschutzverfahren?*




*Schritt 4: Personenbezug*

Ob die ermittelten Verfahren auch datenschutzrelevant sind, ermittle ich im Schritt 4. Jedes dieser Verfahren unterziehe ich einer Analyse, um festzustellen, ob eine Verarbeitung personenbezogener Daten vorliegt.




*Ermittelte Verfahren, in denen personenbezogene Daten verarbeitet werden*

Diese Arbeit erledige ich gern mit einem IT-Verantwortlichen, der neben der Unternehmensstruktur auch die verwendeten Softwareprodukte kennt. Dieses Insiderwissen führt als positiver Nebeneffekt oft zu Anpassungen der ermittelten Verfahren. Aus dem Verfahren „Kundenservice" werden so z.B. noch weitere Verfahren, etwa die Fernbetreuung durch IT-Dienstleistern oder die mobilen Arbeitsplätze.

*Standardverfahren*

Im Schritt 4 füge ich grundsätzlich die Verfahren Büroorganisation und unsere Datenschutz-Dokumentation als Verfahren neu hinzu, da diese Verfahren in jedem Unternehmen anzutreffen sind und personenbezogene Daten verarbeiten.

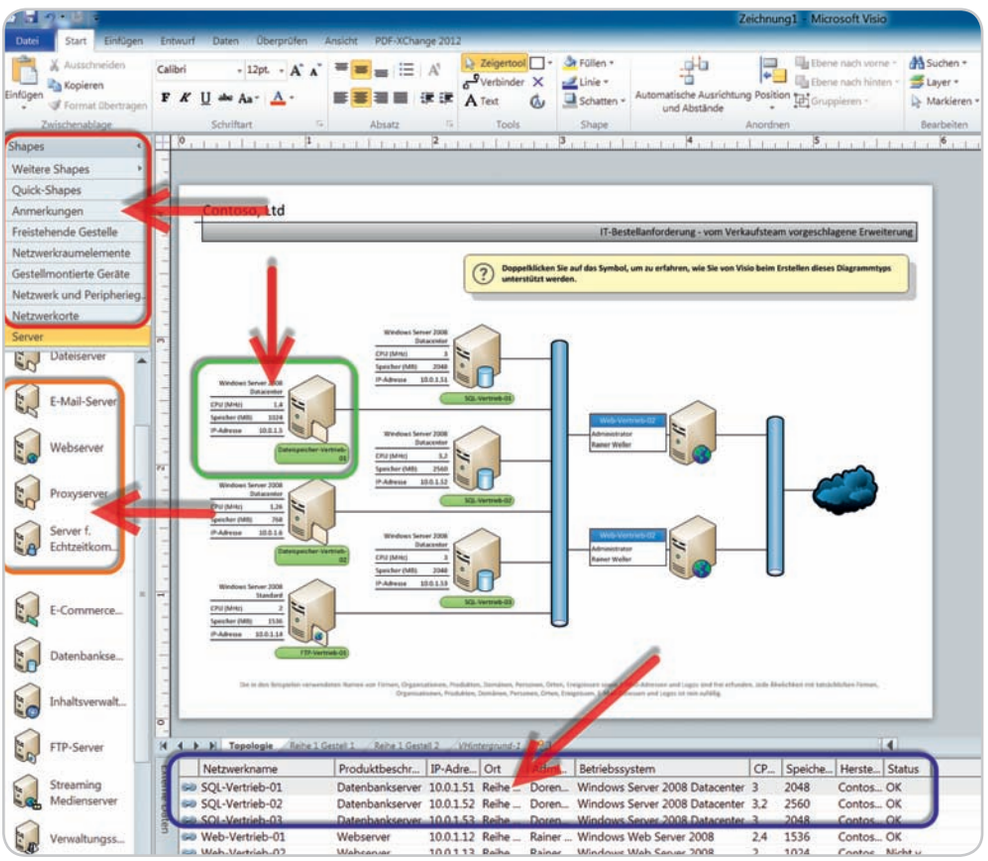
*Tipp*

> In diesem Schritt achte ich auch darauf, dass die Verfahren dem Sprachgebrauch im Unternehmen gerecht werden. Die Prozesse und Strukturen in Unternehmen sind über Jahre gewachsen und in der Umgangssprache der Mitarbeiter verankert. Das ist auch einer der Gründe, warum man Verfahren zwischen den Unternehmen nur selten verallgemeinern kann.

Nach dieser Prüfung verfüge ich nun über eine Übersicht meiner Verfahren in meinem Unternehmen, die mit personenbezogenen Daten zu tun haben:

## IV.2.2 Praxisbeispiel: Eine IT-Landschaft erstellen

Wenn Sie das Register „MS-Vorlage Server-Landschaft“ der Datei „2. Für IT-Darstellungen.vsd“ im Verzeichnis „2. Ihre Datenschutz-Dokumentation\5 Analysen\Muster\Zugaben“ öffnen, erhalten Sie die Ansicht auf die Server einer IT-Abteilung:




*Vorlage für eine Server-Landschaft*

*Tipp*

> Für das Verstehen der Datenschutzzusammenhänge sehe ich IT-technische Details wie Betriebssystem, CPU, Speicher, Festplatte, LAN-Geschwindigkeit, IP-Adresse oder RAID-Verbund nicht als hilfreich an. Wie ein Server heißt und welche Aufgabe er hat, ist für mich dagegen wichtig. Das Abtauchen in die Möglichkeiten des HyperV oder die Backplane einer SAN kann mal interessant sein, um ein besseres Verständnis für die Arbeit der IT zu bekommen, aber für die Datenschutzübersichten eines Datenschutzbeauftragten benötigen wir andere Blickwinkel.

*Mein zweiter Besuch in der Niederlassung*

Bei meinem zweiten Besuch der neuen Niederlassung konzentrierte ich mich auf die IT-Abteilung. Der IT-Leiter nahm ja nebenher die Aufgabe des Datenschutzbeauftragten wahr und fühlte sich in dieser Situation nicht wohl. Bis zur Unternehmensübernahme wurden seine Bedenken jedoch ignoriert.

*Problem: Parallelstrukturen in der IT*

Allmählich erkannte ich Zusammenhänge und stieß auf Merkwürdigkeiten in der IT. Es existierten separate Firewalls, die mit verschiedenen Heimarbeitsplätzen eine Verbindung herstellten. Das Problem bestand darin, dass hier ein zweiter Weg nach außen existierte, von dem der IT-Leiter nichts wusste. Die IT-Mitarbeiter teilten mir mit, dass für diese Komponenten ein externer Dienstleister zuständig sei. Meine Neugier war geweckt. Der Vertrieb hatte an der IT vorbei seine eigene IT-Struktur aufgebaut: drei Vertriebsbüros in größeren Städten, sieben Home-Office-Verbindungen und 15 mobile Zugänge. Von der IT

wurden zehn Home-Office-Zugänge für das Management und 24 mobile Zugänge für die Entwicklungsabteilung betreut. Das roch nach Ärger.

**In drei Schritten zur IT-Übersicht**

Meine Frage nach einer Übersicht endete im Active Directory (Datenbank im Serverbetriebssystem von Microsoft mit Nutzern, Computern, Richtlinien und Organisationsstrukturen). Welche Zugangsberechtigungen nicht mehr genutzt wurden, war auch nicht bekannt. Ich nahm mir vor, in drei Schritten vorzugehen:

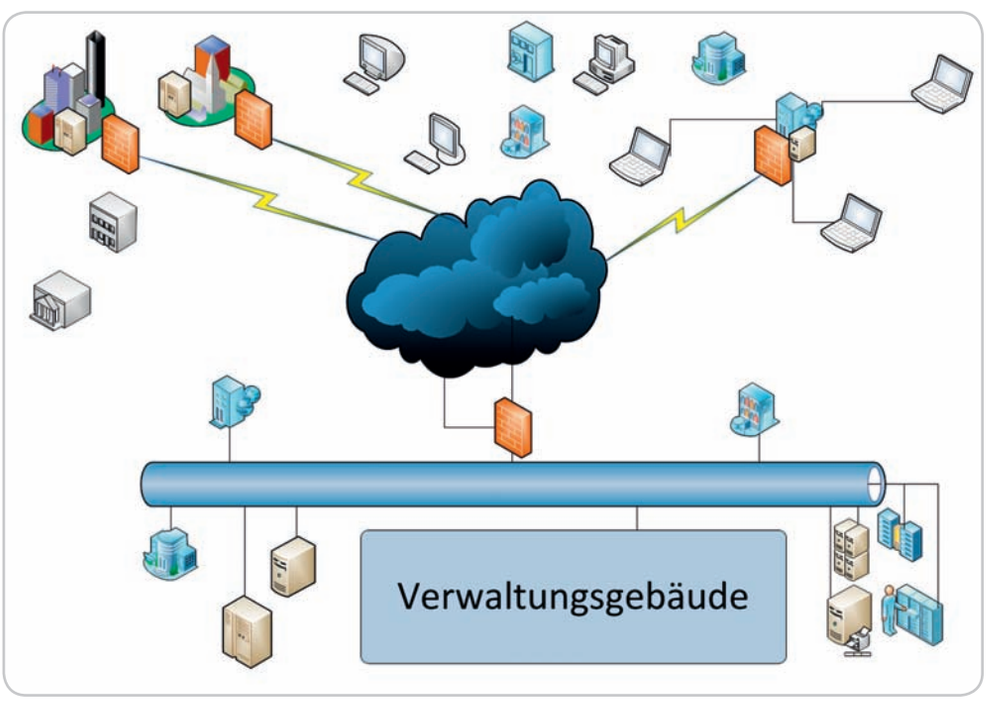
1. Ich wollte mir eine Übersicht verschaffen, wer von wo auf die Daten zugreifen konnte.
2. Die IT bat ich, mir eine Übersicht der genutzten Zugänge zu geben und dann zu veranlassen, dass ungenutzte Zugänge gesperrt wurden.
3. Ich suchte nach einer Lösung, wie sich das Vertriebs- und das Unternehmensnetz verschmelzen ließen.

*Home-Office-Zugänge auflisten – aber wie an Infos kommen?*

Für das Einsammeln der Home-Office-Zugänge half mir wieder Visio. Ich nutzte alle Shapes, die mir dazu einfielen, und bezeichnete jeden Standort, den ich kannte. Meine Vorstellungen waren jedoch das eine, die Umsetzung das andere. Die Informationsbeschaffung war ein zähes Ringen.

Ich suchte nach Unterstützung, und der IT-Leiter bot mir seine Hilfe an. Ich erklärte ihm meine drei Schritte, und er stimmte zu, weil das für ihn schon lange fällig war und in seinen Verantwortungsbereich gehörte. Er gestand mir, dass die Doppelaufgabe IT und Datenschutz ihm aus rechtlicher Sicht Probleme bereitete. Er werde mich daher bei meinem Job als neuer Datenschutzbeauftragter gern unterstützen.

In der Visio-Datei „2. Für IT-Darstellungen.vsd“ finden Sie das Register „Meine erste Server-Landschaft“:




*„Meine erste Server-Landschaft“*

*Eine kleine Übung*

Ihre Aufgabe besteht nun darin, alle Bereiche Ihres Unternehmens in puncto IT-Struktur mittels Shapes abzubilden:

1. Fügen Sie Home Offices, Außenbüros, Niederlassungen, interne Gebäude, Produktionsstätten und Ihre IT-Zentrale in die Zeichnung ein.
2. Vergessen Sie dabei nicht IT-Dienstleister, Steuerberater oder Zulieferer, die über Fernzugriff in Ihr Unternehmen gelangen können.
3. Versuchen Sie, zu verallgemeinern und nicht ins Detail zu gehen. Ein Vertriebsbüro mit sechs PC-Arbeitsplätzen benötigt keine sechs PC-Symbole. Das Verwaltungsgebäude mit 120 Terminalzugängen sollte nicht aus 120 Terminal-Icons bestehen.

Aus Ihren Erkenntnissen bei der Zusammenstellung der IT-Landschaft Ihres Unternehmens ergeben sich zwangsläufig die Darstellungen von Niederlassung, Etagen des Verwaltungsgebäudes oder Abteilungen.

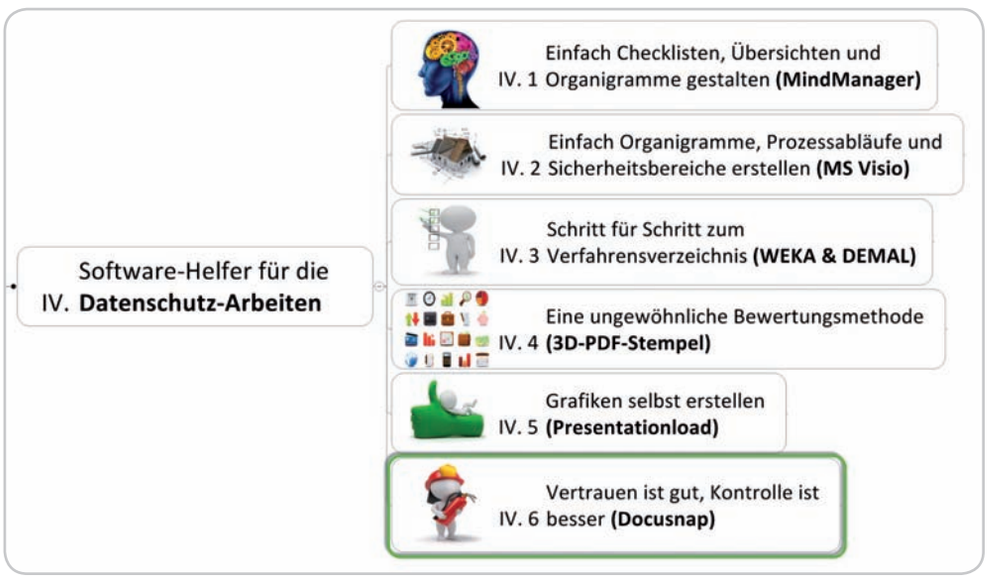
Einem Home Office sollte höhere Aufmerksamkeit zukommen als einem Terminalserverzugang. Ein mobiler Arbeitsplatz muss stärker im Fokus stehen als ein von einer Firewall geschütztes Vertriebsbüro.

*Tipp*

> Nutzen Sie diese Übung, um über Ihr Unternehmen nachzudenken. Wie sich die Shapes auf Ihrer Seite verteilen, ist bei diesem Arbeitsschritt zweitrangig. Es geht um das Einsammeln von wichtigen Informationen.

Wenn Sie der Meinung sind, alle IT-Zugänge erfasst zu haben, gestalten Sie Ihre Zeichnung neu. Nutzen Sie die gesamte Zeichnung und versuchen Sie, zu erreichen, dass ein Betrachter auf den ersten Blick versteht, worum es geht. Vereinfachen Sie Gebäude, Abteilungen oder Rechenzentrum.

# IV.6 Vertrauen ist gut, Kontrolle ist besser (Docusnap)




*Sie befinden sich hier …*

*Jährliche Analyse*

Ich habe es mir zur Regel gemacht, einmal im Jahr die gesamte IT-Landschaft zu untersuchen. Da ich das Ergebnis nur intern für den Datenschutz und die IT nutze, unterstützt mich der IT-Leiter gern bei dieser Analyse und profitiert davon, wenn ich eine Schwachstelle entdecke.

Meines Erachtens ist es wichtig, dass der Datenschutzbeauftragte die Ziele seiner IT-Abteilung unterstützt und dabei den Schutz der personenbezogenen Daten der Mitarbeiter nicht aus den Augen verliert.

**Was erwartet Sie in diesem Kapitel?**

- Ich stelle Ihnen eine Analysesoftware vor, die ich seit Jahren einsetze. Die einfache Nutzung und die schnellen Auswertungen sind eine wirkliche Unterstützung für die Arbeit eines Datenschutzbeauftragten.
- An einem Praxisbeispiel erläutere ich meine Art der Nutzung dieser Auswertungen für interne Audits eines Datenschutzbeauftragten.

*Die goldene Mitte*

Was wäre eine Datenschutz-Dokumentation ohne die Listen aus der IT-Abteilung? Ob diese Listen zu umfangreich sind oder zu wenig IT-Details enthalten, lässt sich nach meinen Erfahrungen nur unbefriedigend beantworten. Im Krisenfall haben mir oft genau die Informationen gefehlt, die der Staatsanwalt haben wollte. Ich werde versuchen, Ihnen einen Mittelweg zu zeigen.

*Der DSB sollte wissen, welche Programme wo laufen*

Interessante Erlebnisse mit Staatsanwälten, Providern, Anwaltskanzleien und Behörden haben bei mir schon früh dazu geführt, dass ich mich intensiv mit IT-Analysen beschäftigt habe, um zu wissen, auf welchem Arbeitsplatz welche Programme installiert sind. Den Erfindungsreichtum der Mitarbeiter und Chefs, die mal schnell einen Film, ein Buch oder Musik im Unternehmen zwischenlagern wollen, sollten Sie nicht unterschätzen!

Eine PC-Auswertung kann schnell 158 Seiten lang sein, und da Ihr Unternehmen „nur" ca. 360 PCs nutzt, könnte die Auswertung zu einem größeren zeitlichen Problem werden. Eine Möglichkeit wäre, diese wichtige Aufgabe als unverhältnismäßig einzustufen und nichts

zu tun. Aber bei der Suche nach einer besseren Lösung stieß ich auf ein Analysewerkzeug aus dem IT-Bereich: Docusnap.

*Was kann Docusnap?*

Nach Hersteller-Angaben erfüllt Docusnap folgende Aufgaben:

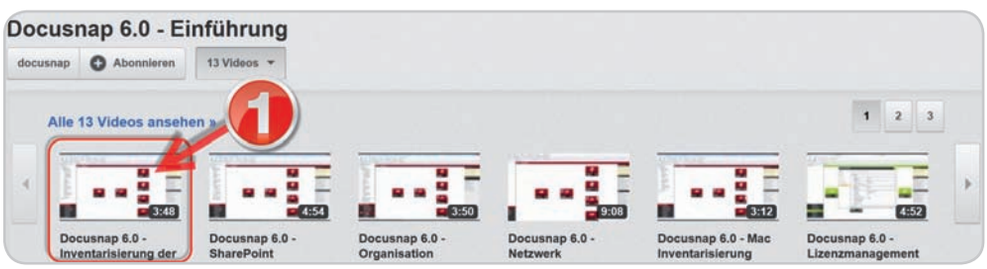
„Die von einer Software gesammelten Daten müssen jederzeit in Plänen, Übersichtslisten, Datenblättern, Diagrammen, Berichten oder z.B. einer Lizenzbilanz für den Benutzer schnell und übersichtlich greifbar sein. Neben den Daten der einzelnen Windows-, Linux- und Mac-Systeme inventarisiert und dokumentiert Docusnap auch das Microsoft Active Directory, die Microsoft-Exchange-, SQL-, DHCP/DNS Server, SharePoint, Hyper-V und VMware-Umgebungen."

*Praktisch für das Berichtswesen des DSB*

Docusnap (www.Docusnap.de) nutze ich seither in verschiedenen Unternehmen zur Vereinfachung meiner Datenschutz- und Auditoren-Tätigkeit. Es handelt sich um ein sehr mächtiges IT-Werkzeug, von dem ich jedoch immer nur die Zusammenfassung der Inventarisierung einsetze. Wenn ein Betriebsrat im jeweiligen Unternehmen vorhanden ist, sollten allerdings im Vorfeld die Belange der Mitbestimmung geprüft werden.

Als Auditor oder bei neuen Mandanten bitte ich die Unternehmen, diese Software einzurichten, um eine unabhängige Überprüfung der IT-Landschaft durchführen zu können. Die Installation ist problemlos. Die erste Einrichtung sollte durch Ihre IT-Abteilung erfolgen, da hier nach Admin-Passwörtern und speziellen IP-Adressen gefragt wird.

Unter http://www.youtube.com/watch?v=3DFdyHRxfnY finden Sie erläuternde Videos zu dieser Analysesoftware. Um schnell zu wissen, worum es bei Docusnap geht, empfehle ich die folgenden zwei Einführungsvideos. Für unsere Zwecke ist das erste Video völlig ausreichend; das zweite zeigt noch weitere Möglichkeiten der Dokumentenerstellung:




*Nur dieses Video ist für dieses Kapitel notwendig*


*Hier finden Sie weiterführende Informationen*

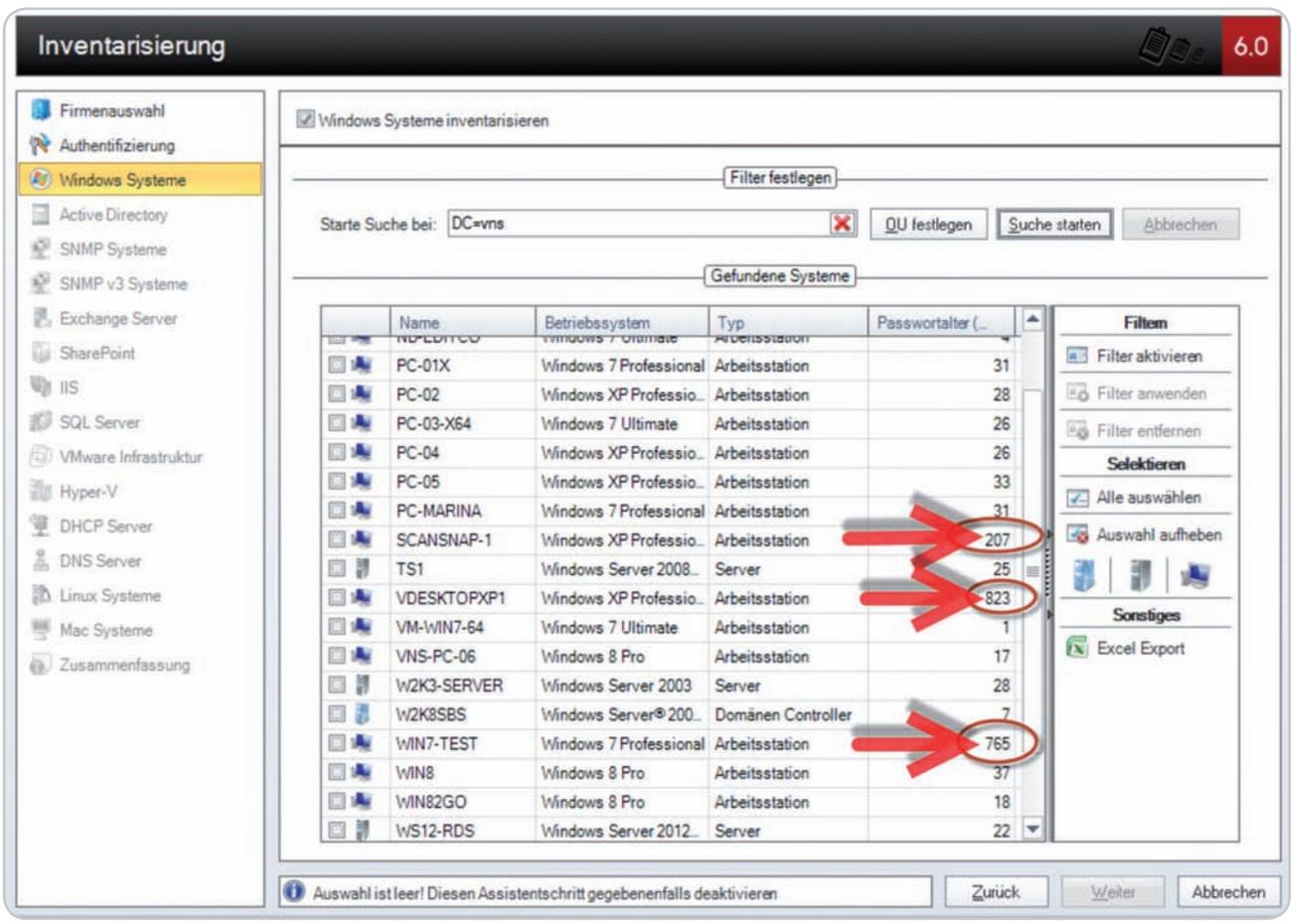
Bei der Nutzung dieses Analysetools gehe ich folgendermaßen vor:

1. Gemeinsam mit der IT richten wir Docusnap ein und lösen den ersten Netzwerkscan aus. Die Einstellungen werden gespeichert. So ist die zukünftige Eingabe von Admin-Passwörtern oder IP-Adressen nicht mehr erforderlich. Bei diesem Vorgang lege ich auch fest, was ich zukünftig im Netzwerk analysieren möchte.
2. Ich bitte die IT, den Docusnap-Server einzurichten, mit dem sich zeitgesteuerte Netzwerkscans durchführen lassen. Die technische Betreuung von Docusnap überlasse ich der IT-Abteilung.
3. Ich nutze dann nur noch die Auswertungen für meine Datenschutzarbeiten oder löse selbst einen Scan aus.

## IV.6.1 Der erste Scan

Der erste Schritt ist für mich sehr wichtig, deshalb möchte ich darauf etwas näher eingehen.

Nachdem die Authentifizierung Ihres Administrators erfolgt ist, beginnt bereits das Abtasten Ihres Netzwerks.




*Information aus dem Active Directory: Passwortalter*

*Passwörter zu alt?*

Am Passwortalter erkenne ich z.B. schon, ob Sicherheitslücken vorhanden sind oder ob die Active Directory (AD) schlecht gepflegt ist. Das Passwortalter ist in Tagen angegeben. Wenn auf einem IT-System ca. zwei Jahre keine Veränderung des Passworts vorgenommen wurde, sollten Sie die Gründe ermitteln.

*Tipp*

Bei Prüfungen externer Unternehmen nutze ich gern als Erstes die Auswertung des Passwortalters, um zu prüfen, wie ernst Datenschutz und Datensicherheit in einem Unternehmen genommen werden.