PRIVAZYPLAN®

Praxisleitfaden für Datenschutz.

Express-Version (Demo)

von SecureDataService
Nicholas Vollmer

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

von
SecureDataService
Nicholas Vollmer

im Mai 2019

Inhaltsverzeichnis

Sie sehen oben, dass die Kapitel 8, 11, 12 und 13 in der "Express"-Version ausgeblendet sind.

… ein ausführliches Inhaltsverzeichnis finden Sie auf Seite 464.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checkliste des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Der Autor:
SecureDataService, Dipl. Ing. (FH) Nicholas Vollmer,
Priorstraße 63, 41189 Mönchengladbach, Deutschland
Tel: +49 2166 96523-38, Fax: +49 2166 96523-39,
E-Mail: n.vollmer@privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel stark gekürzt.

1.1 Vorwort zur aktuellen Ausgabe

Einleitung

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen zur aktuellen Ausgabe im Mai 2019. Was sind die wichtigsten Neuerungen in diesem Monat?

- **Fernzugang statt E-Mails?**
  Es gibt gute Gründe dafür, dass man sensible Informationen und Dateien mit den betroffenen Personen nicht per E-Mail austauscht, sondern mittels Up- und Downloads vollzieht. Dies gilt es zu erwägen. Bitte beachten Sie dabei auch die konkreten Sicherheitshinweise der Aufsichtsbehörden. Seite 22

- **Muss man wirklich ALLE Daten kopieren?**
  Das Recht auf Datenkopie kann im Falle von Beschäftigten sehr viel Arbeit machen. Es empfiehlt sich eine „stufenweise“ Vorgehensweise. Seite 51

- **Kann man eine Datenkopie verweigern?**
  Wann ist ein Verlangen nach Datenkopie „exzessiv“? Unter bestimmten Umständen könnte sich ein Verantwortlich verweigern. Seite 52

- **Zwei wichtige Details zur 72-Stunden-Frist bei Datenschutzverletzungen**
  Für die Meldung an die Aufsichtsbehörde haben Sie (mindestens) zwei Werktage Zeit. Und wenn die Risiken bis dahin beseitigt sind, dann ist wohl gar keine Meldung erforderlich. Seite 148

- **PIA-Tool aus Frankreich ist kritisch zu werten**
  Eine aktuelle Untersuchung betätigt unsere Einschätzung: Das PIA-Tool fokussiert sich zu einseitig auf IT-Sicherheits-Aspekte. Seite 158

- **Deutsches Gesetz zu Geschäftsgeheimnissen**
  Es ist zwar nicht unbedingt datenschutzrelevant, aber das „Geschäftsgeheimnis“ ist nun nicht mehr im UWG behandelt, sondern im neuen „GeschGehG“ Seite 221

- **Statusblatt „Planung für die Planung einer neuen Einwilligung“ wurde ergänzt**
  Es kristallisiert sich heraus, dass die Einwilligungen auf Websites zu Cookies und Tracking einer ziemlich strikten Einwilligung bedürfen. Dies wird nun in diesem Statusblatt berücksichtigt. Seite 278

- **Auch Freelancer sind wohl Auftragsverarbeiter**
  In einer „Baustelle“ wurde thematisiert, ob die DS-GVO möglicherweise eine versteckte Ausnahme für Freelancer kennen könnte. Nach einer längeren Recherche kommen wir zu einem anderen Ergebnis. Seite 381

- **Die Niederlande haben einen Bußgeld-Katalog im Datenschutz**
  Die Niederlande haben den ersten Schritt gemacht. Dem Vernehmen nach arbeiten auch die Deutschen Aufsichtsbehörden daran. Seite 411

- **IP-Adressen sind personenbezogen!**
  Die Deutsche Datenschutzkonferenz stellt nochmals ganz deutlich klar: IP-Adressen sind keine Pseudonyme im Sinne der DS-GVO. Der Datenschutz kommt voll und ganz zum Tragen. Seite 424

- **Sensible Daten per E-Mail versenden**
  Wie sicher sind E-Mails? Was kann man tun? Diese beiden sehr schwierigen Fragen werden ausführlich thematisiert. Möglicherweise ist der „Fernzugang“ eine gute Alternative (siehe oben). Seite 440

- **Wie dokumentiert man Einwilligungen auf der Website?**
  Bisher war nicht klar, wie man auf der Website die Einwilligung für Cookies und Tracking gestalten sollte. Dies dürfte nun geklärt sein. Seite 440

Ich wünsche Ihnen ein gutes Gelingen im Datenschutz…

P.S. in dieser Ausgabe finden sich insgesamt 28 aktualisierte Textstellen. Sie finden alle Stellen, indem Sie nach „Neu im Mail“ suchen. Außerdem gibt es neue Fachliteratur; suchen Sie nach „Neue Literatur“, um diese Stellen zu finden.

1.2 Allgemeines Vorwort (im Mai 2019)

Einleitung

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen.

Bitte erlauben Sie mir hier vorab einige einleitende Worte zur EU Datenschutz-Grundverordnung (**DS-GVO**).

Die Zeit vergeht wie im Flug. Im Januar **2011** präsentierte die EU-Vizepräsidentin (Frau Viviane Reding) in Brüssel den Kommissions-Entwurf einer Datenschutz-Grundverordnung. Seitdem beobachte ich dieses Thema sehr intensiv und berichtete monatlich darüber im TOM-Guide® (siehe hier). Im Frühjahr **2012** hatte sich Jan Philipp Albrecht als Berichterstatter des EU-Parlaments intensiv eingebracht und viel bewegt. Nach turbulenten Verhandlungen zwischen EU-Kommission, EU-Parlament und EU-Rat sah es lange so aus, als würde die DS-GVO niemals kommen. Doch im April **2016** war es völlig überraschend so weit: Europa hat ein neues Datenschutzrecht! In einer kurzen Übergangsfrist von 24 Monaten wird es verbindlich wirksam.

Neu im Mai: **… nun sind wir im Mai 2019** und die DS-GVO hat das erste Jahr hinter sich gebracht. Wie ist der Stand der Dinge?

Seit Juni 2016 stelle ich die Website www.privacy-regulation.eu zur Verfügung, um mir selbst (und meinen Kunden) überhaupt mal den reinen Verordnungstext zugänglich zu machen. Das hat sich als sehr hilfreich herausgestellt. Monatlich verzeichnen wir über 100.000 Besucher. Das ist wohl als ein Erfolg zu werten.

Die große Datenschutz-Katastrophe ist ausgeblieben. Wir hatten 2018 eine beispiellose Einwilligungs-Welle erlebt und die Abschaffung von Klingel-Namensschildern befürchtet. Das ist vorbei. Auch massenhafte Auskunfts- oder sogar Kopie-Verlangen waren nicht zu verzeichnen („Horrorbrief“).
Die Datenschutz-Aufsichtsbehörden haben bisher keine exorbitanten Bußgelder verhängt (von einigen ganz wenigen Ausnahmen abgesehen, siehe Seite 412), und auch die befürchteten Massen-Abmahnungen sind ausgeblieben.

Leider hat die Rechtsunsicherheit zugenommen. Das war auch zu erwarten, denn die unbestimmten Rechtsbegriffe in der DS-GVO sind problematisch. Viele Themen sind extrem strittig (siehe die „roten Bomben“ auf Seite 470). Die deutschen Aufsichtsbehörden veröffentlichen viel Material, aber dadurch wird die Sachlage manchmal sogar noch schwieriger.

Insgesamt stellt die DS-GVO hohe Anforderungen an das Lesepensum eines Datenschutzbeauftragten. Sämtliche Ebenen der Aufsichtsbehörden und EU-Gremien veröffentlichen Entschlüsse, Richtlinien, Orientierungshilfen, Jahresberichte und Positionspapiere. Die 400 wichtigsten Dokumente liefern wir Ihnen ... .

Das stark **überarbeitete Bundesdatenschutzgesetz** (BDSG) im April 2017 quält uns bis heute mit EU-rechtswidrigen Ausnahmen (siehe ab Seite 471). Das deutsche Telemediengesetz (TMG) verschwindet sang- und klanglos. Der deutsche Gesetzgeber zeigt NULL Anstrengung uns die Sachlage klar zu machen.

Die angekündigte ePrivacy-Verordnung lässt noch immer auf sich warten, wodurch viele wichtige Fragen des Internets ungeklärt bleiben (siehe Seite 220).

Mittlerweile hat der **EuGH** eine wichtige Rolle übernommen, um Grundsatzfragen zu klären. Das wird vermutlich weiterhin zunehmen und führt zu jahrelanger Unsicherheit. Wir erinnern uns an „Safe Harbour“, welches quasi über Nacht vom EuGH gekippt wurde.

Doch wo soll man anfangen? Wir liefern Ihnen die 5 wichtigsten Todos!

Und nun, im Mai 2019, wünsche ich Ihnen eine angenehme Lektüre und ein gutes Gelingen!

P.S. Sie haben noch mehr Spaß am PrivazyPlan®, wenn sie unsere „Navigationshilfen im PDF-Dokument“ berücksichtigen.

1.3 Hinweise zum Umgang mit dem PDF-Dokument

Einleitung

Bevor Sie in den fachlichen Teil des PrivazyPlan® eintauchen, möchten wir Sie auf den optimalen Umgang mit dem hier vorliegenden PDF-Dokument hinweisen.

1.3.1 Monatliche Aktualisierung

Dieses PDF-Dokument wird jeden Monat aktualisiert und allen berechtigten Empfängern zugestellt. Diese Vorgehensweise hat sich bewährt, damit alle Leser stets auf dem aktuellen Stand der Dinge sind; unser Datenschutz-Praxishandbuch TOM-Guide® wird seit Mai 2005 auf diese Weise aktuell gehalten. Bezüglich dieser Aktualisierungen gilt Folgendes:

- Im **Vorwort** einer jeden Ausgabe (siehe Seite 5) weisen wir auf die wichtigsten Neuerungen explizit hin. Ein kurzer Erläuterungstext nennt weitergehende Details. Vom Vorwort aus können Sie dann direkt in die neuen Textstellen springen.

- Neuerungen werden gelb **markiert**. Dank der Volltext-Recherchemöglichkeit eines jeden PDF-Readers finden Sie jede Änderung mit einem Klick. Es gibt zwei verschiedene Ansätze bezüglich dieser Markierungen:
  - Umfangreiche Textänderungen werden umfasst von einem „Neu im April: …“ und „ Zurück zum Vorwort “.
  - Kleine Änderungen werden komplett eingefärbt und sehen dann folgendermaßen aus: „Neu im April: Lorem Ipsum dolor sit“.

- **Papierausdrucke veralten** sehr schnell. Bedenken Sie: Wenn Sie den PrivazyPlan® ausdrucken, dann ist der Ausdruck möglicherweise schon nach einem Monat veraltet. Es können neue Texte hinzugekommen sein oder bestehende Texte verändert worden sein. Kapitelnummern und Seitenzahlen können sich ändern. Stecken Sie also nicht zu viel Arbeitsaufwand in handschriftliche Kommentare auf der Papierversion.

Wir haben das **Querformat** für den PrivazyPlan® gewählt, weil wir davon ausgehen, dass viele Leser das Dokument am Computer lesen werden. Insbesondere durch die monatlichen Updates macht der Papier-Ausdruck auf lange Sicht einfach keinen Sinn mehr.

Falls Ihr Papierausdruck am obigen Rand zu viel Text abschneidet, so können Sie in dem PDF-Reader die Ausgabe auf 99% Größe skalieren. Der Text wird dadurch nicht unlesbar.

1.3.2 Navigationshilfen im PDF-Dokument

Der PrivazyPlan® ist mit über 450 Seiten Umfang ein recht großes Dokument. Wie können Sie da noch den Überblick behalten? Hierzu haben wir folgende Tipps:

- Neu im Mai: Wie navigiert und recherchiert man im PrivazyPlan®? In einem Video (12 Minuten) zeigen wir Ihnen alle Tipps und Tricks. Bitte unbedingt anschauen!

- Es stehen **Bookmarks** zur Verfügung. Öffnen Sie in Ihrem PDF-Reader einfach mal die Bookmark-Leiste. Sie werden sehen, dass hierdurch eine Navigation sehr leicht möglich ist.

- Zahlreiche **Inhaltsverzeichnisse** innerhalb des PrivazyPlan® stehen Ihnen zur Verfügung. Mit wenigen Klicks können Sie problemlos zwischen den Kapiteln springen. Wir haben uns hierbei sehr viel Mühe gegeben, damit Sie sich gut zurechtfinden.

- Hilfreiche **Seiten-Verweise** finden Sie überall im Dokument (z.B. „siehe Seite 7„). Diese Seitenzahlen können Sie immer anklicken, um auf die entsprechende Seite zu gelangen. Wir haben diese Seitenzahlen blau gefärbt, damit Sie immer daran denken, dass Sie daraufklicken können.
  ⚠ Wie kommen Sie auf die aufrufende Stelle zurück, wenn Sie auf die Seitenzahl geklickt haben? Ganz einfach: Nutzen Sie die Tastenkombination „ALT+⇦“ um zurück zu springen. Probieren Sie es aus. Dank dieses „Tricks“ können Sie beherzt kreuz und quer springen, ohne den Faden zu verlieren.

  Leider funktioniert das Klicken auf die blauen Seitenzahlen nicht in allen PDF-

Readern gleich gut. Darauf haben wir leider keinen Einfluss. Die Erfahrung hat gezeigt, dass insbesondere die in den Webbrowsern eingebauten PDF-Reader Probleme machen; insofern sollten Sie den PrivazyPlan® dann herunterladen und mit einem „echten" Reader lesen.

- Eine Volltext-**Recherche** ist natürlich ebenfalls möglich. Über die Tastenkombination „STRG+F" öffnet sich in Ihrem PDF-Reader ein Suchfenster. Im „Foxit PDF-Reader" können Sie sich sogar eine Trefferliste anzeigen lassen und sich somit ganz schnell alle Treffer ansehen.

1.3.3 Neues Bundesdatenschutzgesetz ab dem 25.05.2018

In Deutschland gilt ab dem 25.05.2018 ein neues Bundesdatenschutzgesetz.

Die DS-GVO allein ist schon umfangreich und komplex. Doch damit nicht genug, denn die DS-GVO liefert ca. 80 Öffnungsklauseln für nationale Gesetze (siehe Seite 431).

Der Deutsche Bundestag hat diese gesetzgeberische Möglichkeit im April 2017 intensiv genutzt. Es ergeben sich zahlreiche Pflichten für den Verantwortlichen, die im **Kapitel 10** ab Seite 228 beschrieben werden. Weitere Details finden sich im Vorwort des Kapitels **10** auf Seite 229.

Hier im PrivazyPlan® markieren wir die entsprechenden Stellen durch die deutsche Flagge: .

Die Datenschutzgesetze anderer EU-Länder werden nicht in den PrivazyPlan® eingearbeitet.

1.3.4 Welche Bedeutung haben die Hinweise auf den TOM-Guide®?

Parallel zum PrivazyPlan® gibt es noch ein anderes Fachbuch des gleichen Autors: den TOM-Guide®.

Der TOM-Guide® ist ein Praxishandbuch zum Datenschutz mit ca. 700 Seiten Umfang. Dort werden viele Aspekte des Datenschutzes praktisch erklärt.

Der TOM-Guide® steht derzeit nur einem geschlossenen Leserkreis zur Verfügung (nämlich jenen Unternehmen, die im Rahmen von DSB-MIT-SYSTEM® von externen Datenschutzbeauftragten betreut werden).

In einigen Dutzend Fällen verweisen wir hier im PrivazyPlan® auf spezielle Kapitel des TOM-Guide®. Dort werden die entsprechenden Themen vertieft behandelt. Das ist aber für das Verständnis des PrivazyPlan® nicht elementar wichtig.

1.3.5 … so viel Text im PrivazyPlan®, und trotzdem bleiben Fragen…

Trotz des nicht unerheblichen Umfangs von über 330 Seiten ist es dem PrivazyPlan® nicht möglich die ca. 50 Pflichten der DS-GVO bis ins letzte Detail erschöpfend zu beschreiben. Warum ist das so?

Datenschutz ist im Detail komplex. Durch die Aufschlüsselung in ca. 50 Pflichten haben wir die Komplexität der DS-GVO ganz entscheidend verringert. Außerdem beschränken wir uns explizit auf den Bereich der Privatwirtschaft (und ignorieren somit den öffentlichen Bereich). Aber trotzdem bleibt es im Detail manchmal schwierig.

Warum ist die DS-GVO so komplex?

- Die DS-GVO ist **kein harmonisches und ausgereiftes Regelwerk**. Von Januar 2011 bis April 2016 haben in Brüssel die Kommission, das Parlament und der Rat hart verhandelt. Jedes Gremium hat ganz (!) eigene Interessen. Allein im Parlament gab es bis zum Schluss noch 4.000 offene Änderungsanträge. Doch aus politischen Gründen musste der Beschluss im Mai 2017 erfolgen. Also hat man einfach „einen Deckel drauf gemacht". Das spürt man an vielen Stellen.

- Die deutsche **Übersetzung ist nicht immer ganz glücklich**. Bei intensivem Lesen ergeben sich Widersprüche und Ungenauigkeiten. Wir weisen an den entsprechenden Stellen darauf hin (siehe Seite 370). Offensichtliche Übersetzungsfehler und Rechtschreibfehler haben wir korrigiert (und farblich hervorgehoben) auf www.privacy-regulation.eu.

- Viele wichtige **Schlüsselbegriffe** wurden in der DS-GVO nicht definiert. Die Liste der Begriffsbestimmungen im Artikel 4 hätte mindestens dreimal länger ausfallen müssen. Im Ergebnis hantieren Datenschützer mit vielen unbestimmten Rechtsbegriffen (siehe Wikipedia). Manchmal ist das zum Verzweifeln.

- An vielen Stellen ist der **Satzbau** der DS-GVO uneindeutig. Beispielsweise beim Artikel 39 (1b) streiten sich die Fachleute darüber, ob der Datenschutzbeauftragte die Mitarbeiterschulungen durchführen oder nur überwachen soll. Solche Streitfälle wären vermeidbar gewesen, wenn der Verordnungstext in klaren Sätzen formuliert worden wäre. Manchmal hilft ein Blick in die englische Originalversion, um den Sinn zu verstehen.

  Das für Deutschland geltende neue Bundesdatenschutzgesetz ist an vielen Stellen noch viel, viel komplexer formuliert. Manchmal geradezu grotesk. Das gleiche trifft auch für die dazugehörige Gesetzesbegründung zu.

- Die ca. 80 **Öffnungsklauseln** erhöhen die Komplexität (siehe Seite 431). Als hätte die DS-GVO nicht schon genug Regeln, Ausnahmen und Gegenausnahmen zu bieten… nun kommen noch entsprechende Gegen-Regeln mit eigenen Ausnahmen und Gegenausnahmen hinzu. Wo die deutsche Flagge 🇩🇪 ins Spiel kommt, da wird es für die Anwendung in Deutschland nochmal komplexer.

- Nicht zuletzt: **Datenschutz ist ein juristisches – und damit schwieriges - Thema**. Das liegt im Kern ganz einfach daran, dass sich zwei sehr widersprüchliche Interessen gegenüberstehen: **(a)** das Interesse der Unternehmen so viele Daten so flexibel wie möglich zu verarbeiten und **(b)** das Interesse der betroffenen Personen nach Selbstbestimmung und Privatsphäre.
  Das sind die sprichwörtlichen „Äpfel und Birnen", die miteinander verglichen werden müssen. Hierfür braucht es Regeln. Und die sind komplex.

- Die DS-GVO **erscheint irgendwie übertrieben**. Zu hoch erscheinen die Geldbußen, zu umfangreich wirken die Nachweispflichten, zu penibel scheint die Übermittlung in Drittländer geregelt. Warum ist das so? Möglicherweise haben die europäischen Unternehmen dies den US-Giganten wie Facebook, Google etc. zu verdanken.
  Manchmal wirkt die DS-GVO wie ein „**lex facebook**". Viele Regelungen sind erkennbar diesen Internetgiganten auf den Leib geschneidert. Das Problem: Auch alle anderen müssen sich daranhalten.

- Der **Compliance-Virus** befällt nun auch den Datenschutz. Es reicht nicht mehr aus, dass ein Unternehmen „einfach nur Gesetze einhält". Nein, die Einhaltung muss jetzt auch nachweisbar sein. Für die Unternehmen ist das eine Katastrophe: Es gibt immer mehr Regeln und die Einhaltung wird immer schwieriger und aufwändiger. Das Kerngeschäft leidet darunter.
  Der Datenschutz ist hier keine Ausnahme (mehr). Leider. Mit dem PrivazyPlan® möchten wir unseren Teil dazu beitragen, dass Sie sich schnell wieder Ihrem Kerngeschäft widmen können.

- Im August 2017 besteht noch **keine herrschende Meinung** in zentral wichtigen Sachfragen. Es wird noch viele Jahre dauern, bis sich Fachleute, Aufsichtsbehörden und Gerichte einig sind. Bis dahin wird intensiv um „korrekte" Interpretationen gerungen werden. Das erhöht die Komplexität des Themas, weil abweichende Meinungen berücksichtigt werden müssen.

- Insgesamt haben wir festgestellt: Auf jede Antwort gibt es mindestens **zwei Folgefragen**. Es nimmt einfach kein Ende. Fast jeder Sachverhalt hat mehrere Unterfälle und/oder mehrere Interpretationsmöglichkeiten. Je tiefer man fachlich bohrt, desto mehr verliert man sich in komplizierten Details, die keine einfache Antwort mehr zulassen.

Aus diesen Gründen kann der PrivazyPlan® manchmal keine einfache Lösung anbieten. So sehr der Autor das auch bedauert.

Es bleibt unverzichtbar, dass sich die Unternehmen selbst die notwendige Fachkunde aneignen. Daher stellen wir Ihnen im Kapitel 13.3 ab Seite 370 ausführliche **Literatur-Hinweise** zur Verfügung.

Übrigens: Auch als Autor des PrivazyPlan® steht man manchmal vor Rätseln. Als Leser erkennen Sie dies an der roten Bombe:  . Wenn dieses Symbol auftaucht, dann existieren ganz offensichtlich widersprüchliche Interpretationsmöglichkeiten. Eine Zusammenfassung finden Sie auf Seite 470. Wir arbeiten daran, diese fachlichen Unsicherheiten so schnell wie möglich zu beseitigen.

1.4 Wie funktioniert der PrivazyPlan®?

Einleitung

Der PrivazyPlan® ist ein Praxisleitfaden für den Datenschutz gemäß DS-GVO. Im Folgenden beschreiben wir die Grundideen:

Um es vorweg zu nehmen: Letztendlich läuft alles auf **Compliance** hinaus. Wir beschreiben dieses Thema sehr ausführlich auf Seite 359 (mit einer Kurzzusammenfassung auf Seite 366).

Den idealen Einstiegspunkt in die DS-GVO und den PrivazyPlan® erhalten Sie übrigens auf Seite 260.

1.4.1 Den PrivazyPlan® überblicken (Schritt 1)

Sie möchten sich ganz zu Anfang grob in den Pflichten gemäß PrivazyPlan® orientieren? Dann werfen Sie einen Blick in den umfangreichen Anhang. Wir empfehlen die folgende Vorgehensweise:

⚠ Drucken Sie die folgenden Seiten des Anhangs aus:

- die Liste der Verarbeitungsbeispiele ab Seite 315
- die Kurzzusammenfassung aller Pflichten ab Seite 451
- das ausführliche Inhaltsverzeichnis ab Seite 464
- die tabellarische Übersicht aller Pflichten ab Seite 467
- den Index ab Seite 474

… und legen Sie sich diese Ausdrucke griffbereit zur Seite.

Normalerweise würden wir einen Papierausdruck des PrivazyPlan® nicht unbedingt empfehlen, weil er sich bedingt durch die monatlichen Updates ständig ändert. Doch die oben genannten Inhalte sind für den Überblick einfach sehr wichtig.

1.4.2 Den Datenschutz überblicken (Schritt 2)

Vermutlich wollen Sie zunächst erfahren, wo die zugrundeliegenden Gesetzestexte zu finden sind.

Überall im PrivazyPlan® verweisen wir auf die im Folgenden genannten Websites, sodass Sie immer mit einem Klick auf die Originaltexte zugreifen können.

Es lohnt sich, dass Sie in Ihrem Webbrowser die folgenden URLs zu Ihren Favoriten hinzufügen!

a) Die Datenschutz-Grundverordnung (DS-GVO)

Brüssel liefert die **DS-GVO** in Form einer „nackten“ Textdatei. Die 99 Artikel und 173 Erwägungsgründe sind ohne jede Formatierung niedergeschrieben. Es gibt weder Querverweise noch ein Inhaltsverzeichnis.

➔ Unter www.privacy-regulation.eu/de finden Sie eine lesbare Version mit Querverweisen und Vielem mehr. Einen schnellen Zugriff auf die deutsche Version haben Sie über www.gvo2018.de.

➔ Unter www.privacy-regulation.eu/dsgvo-privatwirtschaft.pdf finden Sie eine PDF-Version, die für die Belange der Privatwirtschaft gekürzt wurde.

Ganz besonders stolz sind wir auf die „**Dossier**“-Funktion auf . Wir haben wichtige Kernaussagen mit Schlagworten versehen, auf welche Sie über die Dossiers zugreifen können. Somit werden alle relevanten Verordnungstexte in konzentrierter Form dargestellt. Erst dies erlaubt Ihnen einen übergreifenden Blick auf die Verordnung. Probieren Sie es aus und klicken Sie auf den folgenden Link: “. An vielen Stellen im PrivazyPlan® weisen wir auf diese Dossiers hin.

b) Das neue Bundesdatenschutzgesetz (BDSG)

In Deutschland gilt ab dem 25.05.2018 ein „neues“ Bundesdatenschutzgesetz. Berlin liefert dieses Gesetz in Form eines extrem unübersichtlichen Artikelgesetzes im Bundesgesetzblatt. Auf 36 Seiten findet sich ein Mix aus verschiedenen Gesetzen mit scheinbar ähnlichem Inhalt. Davon sind nur 13 Seiten für die Privatwirtschaft relevant.

➔ Unter www.bdsg2018.de/de finden Sie die relevanten Paragrafen für die Privatwirtschaft.

➔ Unter www.bdsg2018.de/BDSG-privatwirtschaft.pdf finden Sie eine PDF-Version, die für die Belange der Privatwirtschaft gekürzt wurde.

c) Das „alte“ Bundesdatenschutzgesetz (BDSG-alt)

In Deutschland gilt bis zum 25.05.2018 das „alte“ Bundesdatenschutzgesetz. Siehe www.gesetze-im-internet.de/bdsg_1990/index.html. Lassen Sie sich nicht von der Jahreszahl „1990“ irritieren… es handelt sich hier tatsächlich um die aktuelle Version mit der letzten Änderung im März 2017.
Auf der obigen Website finden Sie Hyperlinks auf eine PDF-Version und sogar auf eine englische Übersetzung.

Doch was folgt daraus für Ihr Unternehmen? Das ist Schritt 3…

1.4.3 Ausrichtung nach Pflichten (Schritt 3)

Worum geht es den meisten Unternehmen, wenn sie den Datenschutz einhalten wollen? Sie wollen **Geldbußen vermeiden** (siehe Seite 409). Daher zerlegt der PrivazyPlan® die DS-GVO (inkl. des neuen Bundesdatenschutzgesetzes) in die diesbezüglichen Pflichten.

a) Was sind Pflichten? Wo findet man sie?

Wie kommen wir auf den Begriff „**Pflichten**“? Der Grund hierfür ist der Artikel 39, der sinngemäß fordert:

> *„Dem Datenschutzbeauftragten obliegt die Aufgabe hinsichtlich der **Pflichten dieser Verordnung** zu unterrichten, zu beraten und zu überwachen“.*

Generell sollten alle **relevanten Geldbußen-Bestimmungen** des Artikel 83 (4) und Artikel 83 (5) als „Pflichten“ gelten. Darauf basierend haben wir alle konkret fassbaren Pflichten gesucht, die sich an Formulierungen erkennen lassen wie „… *hat sicherzustellen…*“ oder „… *hat zu dokumentieren…*“. [1]

Auf Seite 409 finden Sie weitergehende Informationen zu Geldbußen, Schadenersatz, Interventionsmöglichkeiten der Aufsichtsbehörden etc.

Wo finden sich die Pflichten in der DS-GVO und dem neuen Bundesdatenschutzgesetz? Werden sie an einer bestimmten Stelle aufgezählt? Nein, so einfach ist das leider nicht. Die Pflichten muss man selbst aus den Texten herauslesen.

Nach intensiver Suche wurden wir an ca. 50 Stellen fündig. Die folgenden Beispiele verdeutlichen dies:

- Artikel 5 (2): „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen** können (Rechenschaftspflicht).“
- Artikel 7 (3): „… Die betroffene Person wird vor Abgabe der Einwilligung hiervon **in Kenntnis gesetzt**...“
- Artikel 8 (2): „Der Verantwortliche [hat sich] **zu vergewissern**, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.“

[1] In Deutschland gelten zusätzlich der § 41 BDG-neu („Anwendung“), § 42 BDSG („Strafvorschriften“) und § 43 BDSG („Bußgeldvorschriften“)

Es haben sich also ca. 50 konkrete Pflichten herausgestellt, die ein Unternehmen auf keinen Fall ignorieren sollte. Auf diese Pflichten konzentriert sich PrivazyPlan®.

Die Identifizierung von Pflichten ist mit **gewissen Unsicherheiten** verbunden. An zahlreichen Stellen in der DS-GVO ist möglicherweise nicht ganz klar, ob es sich dort um eine konkrete Pflicht handeln könnte. An mindestens 21 Stellen in der Verordnung wird beispielsweise ein „Nachweis“ gefordert oder zumindest nahegelegt. An der einen oder anderen Stelle könnte der Leser hier durchaus eine Nachweis-Pflicht erkennen.

[Im Rahmen von PrivazyPlan® wird das angeboten. Dort werden relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, dieses weitreichende Thema besser zu verstehen.]

WICHTIGER HINWEIS: Wir haben die Pflichten der DS-GVO nach bestem Wissen und Gewissen identifiziert. Es mag zukünftig Aufsichtsbehörden geben, die zusätzliche Pflichten identifizieren werden. Insofern geben wir keine Garantie hinsichtlich der Richtigkeit und Vollständigkeit unserer Pflichten-Liste. Durch die monatlichen Updates würden Sie aber von solchen Veränderungen zeitnah erfahren.

b) Jede Pflicht bekommt ein Kürzel

Jede der obigen Pflichten ein **eindeutiges Kürzel**, wie zum Beispiel **[GVO_017a]**. Welche Bedeutung hat das? Wofür ist das nützlich?

- Der **vordere Teil des** Kürzels bezieht sich auf die zugrundeliegende Rechtsvorschrift. Ein „GVO“ steht für die DS-GVO. [2]
  In Deutschland steht ein „BDSG“ für das neue Bundesdatenschutzgesetz.

- Der **hintere Teil** des Kürzels bezieht sich auf die Artikelnummer (bzw. ggf. den Paragrafen). Sollte ein Artikel oder Paragraf mehrere Pflichten aufwerfen, so werden sie alphabetisch durchnummeriert (z.B. „017**a**“).

- Der **Praxiswert** dieser Kürzel ist hoch, da man im Laufe der Zeit viele Kürzel auswendig kennt und somit in den Texten des PrivazyPlan® leichter den Überblick behält. Auch im Gespräch mit Kollegen kann dies ganz erheblich Zeit und Verwirrung (er)sparen, wenn man die Kürzel nutzt, statt immer die Pflicht vollständig zu benennen. Insbesondere bei international aufgestellten Unternehmen überwinden die Pflicht-Kürzel jede sprachliche Barriere.

Die Pflicht-Kürzel werden also nicht einfach nur durchnummeriert (1,2,3, …), sondern orientieren sich an der Artikel- bzw. Paragrafen-Nummer. Wir haben uns für diese Art der Nummerierung entschieden, weil dadurch zukünftige Probleme umgangen werden, wenn neue Pflichten identifiziert werden. Die jetzigen Kürzel werden sich also niemals ändern. Das ist elementar wichtig.

c) Und was ist mit den möglichen Schadenersatzforderungen?

Unabhängig von den Geldbußen drohen natürlich auch Schadenersatzforderungen. Die betroffenen Personen können gemäß Artikel 82 sowohl materielle als auch immaterielle Schäden geltend machen.
Doch lassen sich potenzielle Schadenersatzforderungen im Verordnungstext noch schwieriger eingrenzen als Geldbußen-Gefahren. Im Prinzip kann eine betroffene Person durch „beliebige“ Sachverhalte einen Schadenersatz geltend machen.
Da dies kaum einzugrenzen ist, konzentriert sich der PrivazyPlan® zunächst einmal nur auf die Gefahren von Geldbußen.

Doch wie kann man diese Pflichten besser verstehen, und wo werden die Herausforderungen im Detail erklärt? Das ist Schritt 4…

1.4.4 Pflichten verständlich machen (Schritt 4)

Jede einzelne Pflicht erklären wir ganz konkret. Sie erfahren:

- worin die Pflicht besteht (in wenigen Sätzen zusammengefasst),
- ob das Bundesdatenschutzgesetz ähnliche Pflichten kannte,
- wo die dazugehörige Bestimmung zur Geldbuße zu finden ist (siehe auch Seite 409),
- ob es konkrete Fachliteratur gibt,
- ob in Deutschland das neue Bundesdatenschutzgesetz hier Anwendung findet,
- … und viele wertvolle fachliche Hinweise zu konkreten Fragen der praktischen Bedeutung.

[2] Für die Pflichten des Datenschutzbeauftragten lauten die Kürzel „[DSB_...]“, siehe Kapitel 11 ab Seite 221.

In diesem Sinne wird in den **Kapiteln 2 bis 10** erklärt, was die Pflichten für den Verantwortlichen konkret bedeuten.

Fachlich gesehen kratzen die oben genannten Kapitel natürlich nur an der Oberfläche. Wir möchten auf die **Fachliteratur und Informationsquellen** hinweisen, die das rechtliche Grundverständnis überhaupt erst ermöglicht (siehe Seite 370).

Für wichtige Themen bieten wir auch noch **detaillierte Fachinformationen im** Kapitel 13 ab Seite 355. Wir fassen dort Sachverhalte zusammen, die sehr wichtig sind, und in dieser konzentrierten Form in keinem Fachbuch zu finden sind.

Doch in welcher Reihenfolge können Sie sich den Pflichten widmen? Wie setzen Sie die Prioritäten? Dies ist Schritt 5…

1.4.5 Prioritäten setzen (Schritt 5)

Die ca. 50 Pflichten haben keine feste Priorisierung untereinander. Insofern ist der Verantwortliche zunächst völlig frei in seiner persönlichen Priorisierung.

Auf Seite 16 beschreiben wir ganz ausführlich, wie man die Priorisierung vornehmen kann. Wir liefern Ihnen eine MS-Excel-Tabelle, die Sie nach eigenem Ermessen gestalten können.

Doch wie sollen sie nun konkret in die betriebliche Praxis überführt werden? Dies ist Schritt 6…

1.4.6 Pflichterfüllung organisieren und durchführen (Schritt 6)

In den **Kapiteln 2 bis 10** wird ebenfalls erklärt, wie der Verantwortliche die Pflichten konkret erfüllen kann.

Da bekanntlich ein **Compliance-Managementsystem** angestrebt wird (siehe Seite 359), ist jede Pflichterfüllung zunächst mittels „PLAN, DO, CHECK, ACT“ zu organisieren.

Für jede einzelne Pflicht liefert der PrivazyPlan® deswegen genau diese vier Schritte:

- **PLAN:** Wie will das Unternehmen die jeweilige Pflicht erfüllen? Was ist hier der Selbstanspruch? Welche Priorität wird eingeräumt? Wer ist verantwortlich? Wer ist zuständig? Wie wird der „Erfolg“ der Pflichterfüllung festgestellt? Wie oft soll dies kontrolliert werden? Allgemeine „Plan“-Hinweise finden sich auf Seite 21.

- **DO:** Wie konkret sieht die konkrete Erfüllung der jeweiligen Pflicht aus? Gibt es Arbeitsanweisungen bzw. Checklisten? In einer laufend geführten Dokumentation wird das Maß der Pflichterfüllung dokumentiert. Allgemeine „Do“-Hinweise finden sich auf Seite 22.

- **CHECK:** Im zuvor festgelegtem Zeitintervall wird die jeweilige Pflichterfüllung überprüft. Dies wird schriftlich dokumentiert. Wurden Defizite bei der Pflichterfüllung festgestellt? Allgemeine „Check“-Hinweise finden sich auf Seite 23.

- **ACT:** Wenn es Defizite bei der jeweiligen Pflichterfüllung gibt, so muss der jeweils verantwortliche Mitarbeiter darüber informiert werden. Er entscheidet darüber, ob es Handlungsbedarf gibt. Gegebenenfalls muss die Planung überarbeitet werden. Allgemeine „Act“-Hinweise finden sich auf Seite 23.

Der PrivazyPlan® hat den Anspruch, dass die obigen Punkte für alle ca. 50 Pflichten konzipiert sind. Das Unternehmen kann also sofort mit der konkreten Bearbeitung beginnen.

Vermutlich wird es vor allem das „DO“ sein, welches das Unternehmen vor zeitliche und inhaltliche Herausforderungen stellt.

Zahlreiche **Formular-Beispiele** finden sich im **Kapitel 12** auf Seite 258. Hier finden Sie präzise Anregungen, wie sie einige Pflichten konkret erfüllen können.

1.4.7 … und die Pflichten des Datenschutzbeauftragten?

Im **Kapitel 11** beschreiben wir die **acht Pflichten des Datenschutzbeauftragten** (siehe Seite 247-258).

Diese Pflichten ergeben sich aus Artikel 37, Artikel 38 und Artikel 39.

Die Pflicht zur Benennung eines Datenschutzbeauftragten ergibt sich zunächst aus dem Artikel 37 (1) und betrifft (vereinfacht gesagt) nur jene Unternehmen, deren **Kerntätigkeit** in Art oder Umfang besonders in die Rechte und Freiheiten der betroffenen Personen eingreift.

In Deutschland gilt gemäß § 38 BDSG u.a. eine Benennungspflicht, wenn mindestens **zehn Personen** ständig mit der automatisierten Datenverarbeitung beschäftigt sind (also z.B. über persönliche E-Mail-Adresse verfügen). Siehe Seite 196.

Sollte Ihr Unternehmen **keinen** Datenschutzbeauftragten bestellen (müssen), dann muss jemand anders im Unternehmen diese Pflichten wahrnehmen (um z.B. als Anlaufstelle für Aufsichtsbehörden dienen).

1.5 Wichtige Entscheidungen vorab

Im Unternehmen müssen einige ganz grundsätzliche Entscheidungen erfolgen. Die Wichtigsten wollen wir hier kurz thematisieren. Sie werden sehen, dass diese Fragestellungen recht komplex sind; es ist nicht zu erwarten, dass Sie die Antworten hier und jetzt finden müssen. Doch behalten Sie im Hinterkopf, dass diese Fragen irgendwann relevant werden. Ihr Datenschutzbeauftragter wird Sie sicherlich gerne beraten.

Die Ergebnisse Ihrer Überlegungen können Sie beispielsweise in der **Datenschutz-Leitlinie** hinterlegen (siehe Seite 273).

1.5.1 Welches Compliance-Managementsystem passt zu Ihnen?

Bekanntlich ist der Datenschutz ein **Compliance**-Thema (siehe Seite 359).

Treffen Sie eine Entscheidung: Wie soll in Ihrem Unternehmen die Datenschutz-Compliance organisiert werden? Möchten Sie alle Dokumente und Todos mit MS-Word und MS-Excel realisieren? Oder wollen Sie möglicherweise einen MS-Sharepointserver verwenden, um die zahlreichen Informationen handhabbar zu machen? Oder wollen Sie sich eine kostenintensive und professionelle Software anschaffen?

1.7 Allgemeine Bearbeitungshinweise (zum PDCA-Zyklus)

Einleitung

In den **Kapiteln 2 bis 10** wird angeleitet, wie der Verantwortliche die ca. 50 Pflichten erfüllen kann. Dabei gibt es gemeinsame Aspekte bei allen Pflichten.

Da bekanntlich ein **Compliance-Managementsystem (CMS)** angestrebt wird (siehe Seite 359), ist jede Pflichterfüllung zunächst mittels „PLAN, DO, CHECK, ACT“ zu organisieren. Dies ist der bekannte PDCA-Zyklus.

Es hat sich gezeigt, dass es im PrivazyPlan® bei den ca. 50 Pflichten immer wieder identische Überlegungen gibt. Um ständige Wiederholungen zu vermeiden (und Platz zu sparen) werden diese Überlegungen hier zusammengefasst.

In allen vier Phasen des PDCA-Zyklus werden Sie die Aufforderung finden, dass **ein neues Dokument erstellt** werden muss. Dies ist natürlich nur eine unverbindliche Empfehlung. Sie entscheiden selbst, wie Sie Ihr CMS organisieren: In MS-Word oder in einer spezialisierten Software oder in Form eines Ticket-Systems. Siehe die diesbezügliche generelle Überlegung auf Seite 417.

⚠ Wenn Sie die Pflichten später konkret bearbeiten, so macht es Sinn, dass Sie sich die folgenden drei Seiten ausdrucken und bereithalten. Auf diese Weise können flüssig arbeiten.

1.7.1 Allgemeine Planungshinweise („plan“)

In jeder Pflicht der Kapitel 2 bis 10 gibt es die Planungsphase („plan“). Bestimmte Überlegungen zur jeweiligen Pflicht sind immer identisch. Diese Überlegungen sollen hier vorab aufgeführt werden:

1.8 Systematische Kürzel für Einwilligungen und Infotexte

Einleitung

Der Verantwortliche wird im Rahmen der DS-GVO viele Einwilligungs- und Informationstexte erstellen (und beständig aktualisieren). Das kann eine komplizierte Angelegenheit werden, wenn man bedenkt, dass es langfristig von großer Wichtigkeit sein kann, WANN das Unternehmen WELCHEN Text WO nutzte.

Beispiel: Eine betroffene Person bestreitet, dass sie vor drei Jahren konkret der Daten-Offenlegung an Facebook eingewilligt habe. Die Person behauptet, dass niemals von Facebook die Rede gewesen wäre. Der Streitfall liegt bei der Aufsichtsbehörde, die jetzt vom Unternehmen einen präzisen Einwilligungs-Nachweis vom 14.04.2013 fordert. Was tun?

Dieser Art von Problematik kann man auf einheitliche Weise begegnen. Die fraglichen Texte zur Einwilligung bzw. zur Betroffenen-Information erhalten ein **eindeutiges Kürzel**:

- Einen Bezeichner wie „e“ für Einwilligung oder „i“ für Informationstext.
- Eine laufende Nummer wie „001“ die hochgezählt wird.
- Eine Revisionsnummer für leichte inhaltliche Änderungen wie „a“, „b“ oder „c“
- Ein Kürzel für die Landessprache wie „de“ oder „en“

Der erste Einwilligungstext in deutscher Sprache hätte also das Kürzel „e001_de“. Wird er geringfügig überarbeitet, so ändert sich das Kürzel auf „e001**a**_de“. Wird er ganz grundsätzlich überarbeitet, so sollte eher die laufende Nummer erhöht werden.

Diese Kürzel könnte man vielfältig verwenden:

- Man könnte sie als Kürzel in eckigen Klammern hinter die Textveröffentlichung hinzufügen („[E001a_de]“), wodurch sie auf dem jeweiligen Formular (oder Webseite) immer leicht zu identifizieren ist. Sollte dieses Kürzel fehlen, so könnten „Insider“ sofort erkennen, dass dies möglicherweise ein nicht-kontrollierter Text ist.
- In einem konkreten Einwilligungsnachweis gemäß Pflicht [GVO_007] auf Seite 121 müsste man nicht immer den vollen Wortlaut dokumentieren (und zwar in der jeweiligen Landessprache), sondern man bräuchte nur das Kürzel erwähnen. Sehr praktisch!
- Durch diesen systematischen Umgang kann man der Aufsichtsbehörde sehr effizient nachweisen, dass man die Thematik der Einwilligungen ernst nimmt. Diese Tatsache wird bei der Höhe einer potenziellen Geldbuße bestimmt positiv gewürdigt.
- Auf der Firmen-Website kann man den Einwilligungstext publizieren, indem man das Kürzel als Dateinamen nutzt (z.B. „**e001a_de.htm**“). Dies ist gemäß Erwägungsgrund 58 eine zulässige Maßnahme, um für Transparenz zu sorgen. Dies ist insbesondere dann eine gute Maßnahme, wenn die Einwilligungs-Modalitäten z.B. nicht auf eine Postkarte passen. Dies gilt natürlich nur für den Fall, dass die Adressaten absehbar Internet-affin sind.

Solch ein systematischer Ansatz zwingt das Unternehmen quasi zur zentralen Ablage aller Einwilligungen und Informationstexte. Genau das ist der richtige Weg! Sie könnten hierfür z.B. die folgende Speicherung vorsehen:
`\PrivazyPlan\Einwilligungen\e001a_de.docx`

Zugegeben: Dies ist ein sehr ungewöhnlicher Weg, um die Einwilligungs- und Informationstexte zu kontrollieren. Aber gibt es eine Alternative?

Die Speicherung sollte an zentraler Stelle in einem Dokumenten-Managementsystem auf revisionssichere Weise erfolgen und für alle relevanten Kollegen zugreifbar sein (siehe Seite 418).

Diese hier beschriebenen Kürzel sind ein guter Ansatz, um die Forderung der Artikel-29-Datenschutzgruppe auf Seite 20 des Workingpaper „WP 259“ zu erfüllen: „*The controller could retain a copy of the information that was presented to the data subject at all time*“.

1.9 Was leistet der PrivazyPlan® nicht?

Einleitung

Der PrivazyPlan® ist **kein** klassisches Fachbuch.

Ein „normales“ Fachbuch zur DS-GVO hat meist den Anspruch die gesamte Verordnung in all ihren Aspekten zu beleuchten.

Doch der PrivazyPlan® betrachtet **nur die Pflichten, die der Gefahr einer Geldbuße** unterliegen. Somit werden nur ca. 30 von 99 Artikeln der DS-GVO hier thematisiert. Die anderen Artikel finden (fast) keine Erwähnung.

Außerdem werden sämtliche Bestimmungen des öffentlichen Bereichs ausgeklammert. Somit richtet sich der PrivazyPlan® ganz gezielt nur an die Privatwirtschaft.

Der PrivazyPlan® ist kein zertifizierbares Datenschutz-Managementsystem. Zwar werden die Datenschutz-Pflichten erklärt und mit Checklisten versehen, aber eine vollständige Anleitung zur innerbetrieblichen Organisation findet sich nicht. In dieser Hinsicht sei beispielsweise auf die VdS-Richtlinie 10010 hingewiesen.

Doch wo finden Sie klassisches Fachwissen?

- Übergreifendes Fachwissen finden Sie im Kapitel 13 („Fachinformationen“) ab Seite 355.
- Umfangreiche Tipps zu Fachbüchern und Onlinequellen finden Sie ab Seite 370.

1.10 Datenschutz-Managementsystem mit minimalen Mitteln („Mini-DSMS“)

Einleitung

Sie möchten ein Datenschutz-Managementsystem („DSMS“) in Ihrem Unternehmen ganz konkret realisieren? Selbstverständlich gibt es dafür hochspezialisierte Softwareprodukte (wie beispielhaft auf Seite 364 beschrieben). [5] Aber es geht auch simpler:

➔ Unter finden Sie unseren Minimal-Vorschlag.

Mit diesem von uns vorgeschlagenen „Mini-DSMS“ können Sie alle Pflichten des PrivazyPlan® in die Praxis umsetzen. Sie benötigen lediglich ein Tabellenbearbeitungsprogramm. Zusammen mit der VdS-Richtlinie 10010 (siehe Seite 367) lässt sich die DS-GVO sehr gut in die Praxis umsetzen.

Unser Ansatz basiert auf drei grundlegenden Ideen:

1. Für jede Pflicht des PrivazyPlan® wird ein **Unterverzeichnis** erstellt. Dort können alle Dokumente zu dieser jeweiligen Pflicht abgelegt werden.
2. **Dokumente aller Art** können im Unterverzeichnis „*_Allgemeines*“ gespeichert werden, sofern sie pflichtübergreifend relevant sind.
3. Auch die Dateien **PrivazyPlan.xlsx** gehört zu diesen übergreifenden Dokumenten. Hier können die Pflichten bearbeitet werden und der Fortschritt dokumentiert werden.

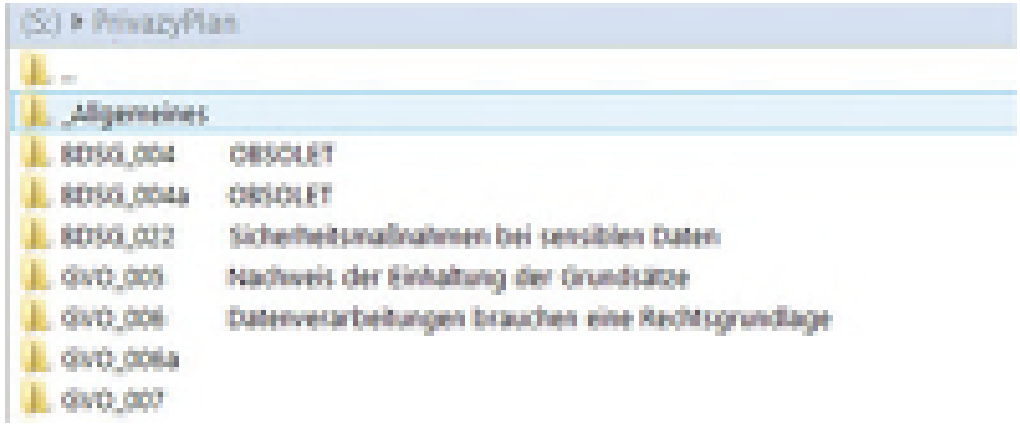
Dies soll im Folgenden erläutert werden:

1.10.1 Zu 1: Ein Unterverzeichnis für jede Pflicht

Im Laufe der Zeit wird es viele Dokumente geben, die zu einer konkreten Pflicht gehören. Dies können sein: Fachliteratur, Arbeitsanweisungen, Checklisten, Testate, Einwilligungstexte und vieles mehr.

[5] Im Englischen verwendet man den Begriff **Privacy Information Management System** („PIMS“). Diesbezüglich ist eine internationale Standardisierung geplant; die ISO/IEC sieht ein Datenschutz-Managementsystem als Erweiterung des ISMS an (siehe Seite 133). Eine entsprechende Norm ISO/IEC 27552 ist in Arbeit (siehe Seite 358). Das Fachbuch „Privacy Impact Assessment“ thematisiert diesen Aspekt im Kapitel 2.4 (siehe Seite 155).

Deswegen beinhaltet die PrivazyPlan.zip für jede Pflicht ein eigenes Unterverzeichnis. Dies sieht prinzipiell folgendermaßen aus:



Hier können Sie ggf. auch die Dokumente zum PDCA-Zyklus speichern, so wie es bei den allgemeinen Bearbeitungshinweisen auf Seite 21 beschrieben ist. Auch die Formulare des Kapitels 12 (ab Seite 258) können hier gespeichert werden; die entsprechenden Dateinamen werden in den jeweiligen Unterkapiteln bereits vorgeschlagen.

\PrivazyPlan\GVO_005
… auf diese Weise erkennen Sie überall im PrivazyPlan®, dass wir auf genau diese Verzeichnisstruktur verweisen. Links findet sich das gelbe Folder-Symbol und rechts daneben in blauer Schrift nennen wir das jeweils passende Unterverzeichnis.

Die Verzeichnisnamen tragen nicht nur das Kürzel, sondern zusätzlich auch die Überschrift der jeweiligen Pflicht. Im Oktober 2018 sind viele hilfreiche Unterverzeichnisse und „_liesmich.txt“-Dateien hinzugekommen. Außerdem wurden einige Formulare und Checklisten aus dem hier vorliegenden PrivazyPlan® in ein MS-Word-Dokument übernommen, um es leicht bearbeiten zu können.
Zu 2: Ein Unterverzeichnis für Dokumente aller Art
Sie werden allgemeine Dokumente im Rahmen des PrivazyPlan® speichern wollen. Dafür finden Sie Platz in dem Verzeichnis „*_Allgemeines*“.

Hier können Sie beispielsweise auch Fachliteratur speichern, wie beispielsweise das empfehlenswerte eBook „DS-GVO im Überblick“ in Deutsch und Englisch (siehe Seite 260). Der PrivazyPlan® liefert hier auch eine Mindmap-Grafik zu allen Pflichten (siehe Seite 473).

1.10.2 Zu 3: PrivazyPlan.xlsx

Diese MS-Excel-Tabelle befindet sich im ZIP-Unterordner **_Allgemeines** und kann Ihnen helfen die Pflichten zu priorisieren und zu bearbeiten.

In dieser Demo-Version sind die restlichen Inhalte ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version wurde alles außer Kapitel 2.1 ausgeblendet. Allerdings finden Sie im Kapitel 2.1 viele wertvolle Hinweise auf die wichtige Pflicht zur Information der betroffenen Personen.

2.0 Einleitung

Persönlichkeitsrechte

In diesem Kapitel werden alle Pflichten beschrieben, die mit den Persönlichkeitsrechten der betroffenen Personen zu tun haben; siehe Kapitel III der DS-GVO in den Artikeln 12-23.

Diese Pflichten sind wichtig, weil der Verantwortliche hier für viel Transparenz sorgt, und sich die betroffenen Personen demzufolge sehr einfach beschweren können und sogar Schadenersatz fordern können.

Die Aspekte der Persönlichkeitsrechte werden auch in der VdS-Richtlinie 10010 (siehe Seite 367) im dortigen Kapitel 10.12 („Betroffenenrechte“) thematisiert.

➔ Die allgemeinen Erwägungen zur Gewährleistung der Persönlichkeitsrechte sind in der Checkliste „**Allgemeine Bearbeitungshinweise (zum PDCA-Zyklus)**“ zusammengefasst (siehe Seite 21). Jenes Kapitel ist von entscheidender Wichtigkeit!

In den folgenden Kapitel beginnt jede Pflicht auf einer neuen Seite, damit Sie diese bei Bedarf gezielt ausdrucken können.

2.1 Bei Erhebung von Daten ausführlich informieren [GVO_013]

Persönlichkeitsrechte

Gemäß Artikel 13 (1) und Artikel 13 (2) muss das Unternehmen die betroffenen Personen schon bei der Datenerhebung sehr ausführlich informieren. Dies soll die Fairness und Transparenz der Verarbeitung sicherstellen. Man könnte diese Information als eine Art „Beipackzettel“ ansehen. [6]

Dieser Pflicht wird das Kürzel **[GVO_013]** zugeordnet (siehe Seite 12).

2.1.1 Allgemeine Informationen zur Pflicht [GVO_013]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 409). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) gab es keine derartigen Pflichten.

In der **Fachliteratur** (siehe Seite 370) gibt es viele hilfreiche Dokumente: ● 40-seitige Orientierungshilfe aus Bayern ● Ausführliche Hinweise in der ULD-Praxisreihe 4 auf 18 Seiten. ● Die Aufsichtsbehörde in Brandenburg bietet ein Informationsblatt ● DSK-Kurzpapier-10 ● Die 11-seitige GDD-Praxishilfe DS-GVO VII („Transparenzpflichten“). ● Trainingseinheit 6 („Betroffenenrechte und Informationspflichten“) der Informationsreihe „Fit für die Datenschutz-Grundverordnung“.

2.1.2 Was bedeutet diese Pflicht [GVO_013] ?

a) Was ist eine Erhebung von Daten? Wann muss man informieren?

Für den Begriff „**Erhebung** von Daten“ (engl. „collect“) liefert die DS-GVO im Artikel 4 leider keine Definition. In Deutschland lieferte der § 3 Abs. 3 BDSG-alt diese Definition: „*Erheben ist das **Beschaffen** von Daten über den Betroffenen*“. Es ist wohl davon auszugehen, dass hier eine AKTIVITÄT des Verantwortlichen vorliegen muss (siehe hier und hier und hier in RdNr. 15-16) . [7] Dementsprechend fallen unverlangt zugesendete Daten vermutlich nicht unter diese Informationspflicht.

Leider ist die Sachlage nicht besonders klar. Es besteht stets die Gefahr, dass eine betroffene Person (oder ein Wettbewerber) hier eine unterlassene Information wittert und sich beschwert bzw. eine Abmahnung ausspricht (siehe Seite 415).

Was bedeutet das in der Praxis? Am Beispiel von Visitenkarten kann man wohl von zwei typischen Szenarien ausgehen:

1. Der Verantwortliche stellt auf einer Messe eine **Visitenkarten-Sammelbox** auf, wo die Messebesucher Ihre Visitenkarten einwerfen können. Es ist geplant, dass diese Daten in einer Customer-Relation-Management-Software (CRM) gespeichert werden. Es handelt sich hier also ganz klar um eine zielgerichtete Datenerhebung. Die betroffenen Personen müssen also informiert werden.

2. Der Verantwortliche **erhält beiläufig die Visitenkarten** von Gesprächspartnern im Rahmen von Messe-Gesprächen. Das Ziel ist eine mehr oder weniger diffuse Kontaktaufnahme, um über Geschäftsanbahnung zu sprechen. Dies ist keine gezielte und zielgerichtete Erhebung und bedarf keiner Information. Siehe auch die entsprechende FAQ-11 der Bayerischen Datenschutz-Aufsichtsbehörde.

Ein anderes Beispiel liegt bei der telefonischen Datenerhebung vor. Auch hier gibt es zwei verschiedene Szenarien:

1. Der Verantwortliche richtet eine **Telefonnummer für Gewinnspiele** ein, wo Personen ihre Daten nennen können. Es ist klar, dass hier gezielt Daten erhoben und genutzt werden. Dies ist ganz klar informationspflichtig.

2. Auf der normalen Geschäftsnummer **nennt eine Person ungefragt Daten**. Zum Zeitpunkt des Gesprächs lässt sich noch gar nicht vollständig bestimmen, ob und wo die Daten gespeichert werden. Erwartet die DS-GVO, dass wir jeden

[6] Frei nach dem Motto: „*Zu Risiken und Nebenwirkungen dieser Daten-Erhebung fragen Sie den Verantwortlichen oder seinen Datenschutzbeauftragten*“.

[7] Siehe auch im BDSG-Kommentar von Gola/Schomerus in RdNr. 23 zu § 3 BSG-alt (sinngemäß: „Gemeint ist jedoch ein zielgerichtetes Beschaffen der Daten durch die verantwortliche Stelle. Bei zufälligen Beobachtungen oder unaufgeforderten Zuleitungen wird nicht ‚erhoben‘“.

Anrufer über mögliche (digitale) Gesprächsnotizen informieren müssen? Das ist wohl eher nicht zumutbar.

In der Fachzeitschrift ZD 11/2018 Seite V-VII wird ebenfalls auf die „Erhebung" eingegangen (incl. Visitenkarten-Übergabe: „*Bei der Übergabe einer Visitenkarte handelt es sich um **keine** Datenerhebung, wenn ein sozialadäquates oder gar gesellschaftlich gebotenes Alltagsverhalten vorliegt, dem keine Datenverarbeitungsmotivation entnommen werden kann*").

b) Worüber muss man informieren?

Im Vergleich zum § 34 Abs. 1 BDSG-alt müssen sehr viel mehr Details offengelegt werden; außerdem muss diese Information ungefragt (!) geliefert werden. Insofern ist diese DS-GVO für die betroffenen Personen ganz unmittelbar spürbar: Wann immer Daten erhoben werden sollen, so wird zuvor eine lange Liste an Informationen geliefert. Es gibt keine Datenerhebung „ins Blaue" mehr. Die betroffenen Personen sind von Anfang an sehr gut informiert; daher ist mit mehr Rückfragen oder kritischen Anmerkungen zu rechnen. Teilweise wird der Verantwortliche so manches Detail offenlegen müssen, welches er eigentlich nicht gerne offenbart (weil er befürchtet, dass so manche Person die Verarbeitung ihrer Daten verweigern würde oder auf die Eingabe freiwilliger Details verzichten würde).

⚠ Ein absolutes Novum ist das Detail in Artikel 13 (1d): Die „berechtigten Interessen" des Verantwortlichen müssen mitgeteilt werden. Hier erkennt die betroffene Person also ganz genau den Zweck bzw. die „Motivation" der Verarbeitung. Das macht die Datenverarbeitung in besonderem Maße „angreifbar", weil dieser Erlaubnistatbestand des Artikel 6 (1f) keine überwiegenden Interessen der betroffenen Personen toleriert, und dementsprechend die betroffenen Personen gemäß Artikel 21 (1) widersprechen können (und die Daten bis zur Klärung der Sachlage gemäß Artikel 18 (1) zunächst einmal eingeschränkt werden, siehe Seite 66).
Im Verarbeitungsverzeichnis gemäß Artikel 30 sollte demnach die Rechtsgrundlage einer Verarbeitung dokumentiert werden.

Neu ist auch die Forderung, dass die Kontaktdaten des Datenschutzbeauftragten gemäß Artikel 13 (1b) schon zum Zeitpunkt der Datenerhebung mitzuteilen sind. Das „Schattendasein" des Datenschutzbeauftragten hat somit ein Ende. Es ist zu hoffen, dass sich unzufriedene betroffene Personen demnach zunächst beim Datenschutzbeauftragten melden, bevor sie sich bei der Aufsichtsbehörde beschweren.

Die Aufspaltung der Informationspflicht des Artikel 13 in die Absätze 1 und 2 ist verwunderlich und hat wohl eher historische Gründe (siehe Kühling/Buchner in RdNr. 20f zu Artikel 13). Der Verantwortliche macht nichts falsch, wenn er immer alle Informationen beider Absätze liefert.

Tipp: Diese Informationspflicht sollte unbedingt beachtet werden, weil eine Missachtung sofort auffällt. Sowohl die betroffenen Personen als auch die Aufsichtsbehörde, als auch die Konkurrenz (!) wird das Fehlen sofort bemerken. Die Gefahr von Geldbußen, Schadenersatzforderungen und Abmahnungen ist hoch (siehe Seite 409).

c) Wann muss man NICHT informieren?

Der Erwägungsgrund 62 schränkt ein, dass sich das Informationsrecht erübrigt, wenn **(a)** die Person bereits über diese Information verfügt oder **(b)** die Verarbeitung ausdrücklich durch eine Rechtsvorschrift geregelt ist oder **(c)** die Mitteilung unmöglich ist bzw. einen unverhältnismäßig hohen Aufwand erzeugt.

Diese Ausnahmen sind natürlich mit zahlreichen Fragezeichen versehen. Außerdem könnte eine betroffene Person (bzw. ein Wettbewerber) mangels Kenntnis dieser Regelung einen Datenschutzverstoß wittern und sich beschweren (bzw. eine Abmahnung aussprechen, siehe Seite 415).

d) Muss man die Informations-Erteilung im Einzelfall dokumentieren?

Der Artikel 13 nennt **keine Pflicht zum dauerhaften Nachweis** von erteilten Informationen. Die betroffene Person könnte somit jederzeit bestreiten eine Information erhalten zu haben. Liegt die Beweislast hier beim Verantwortlichen?

Um einen präzisen Nachweis einer Informations-Erteilung geben zu können, müsst jede Person vor der Informations-Erteilung zuverlässig identifiziert werden. Nur dann hätte der Verantwortlich eine genaue Kenntnis, wen er da mit Informationen versorgt hatte. Das wäre für beide Seiten eine Zumutung. Dies lässt sich auch dem Erwägungsgrund 57, Erwägungsgrund 64 und Artikel 11 entnehmen.

Hinzu kommt der Grundsatz der **Datenminimierung** gemäß Artikel 5 (1e). Es kann nicht im Sinne der DS-GVO sein, dass man jede einzelne Informations-Erteilung jahrelang personenbezogen speichert.

Unbedenklich wäre hingegen ein rein organisatorischer Ansatz: Überall, wo eine aktive Datenerhebung stattfindet, dort können die Beschäftigten angewiesen werden eine Information zu liefern. Eine sorgfältige Planung und eine gewissenhafte

Dokumentation könnten ausreichen, um die betroffenen Personen und die Aufsichtsbehörde (und ggf. ein Gericht) zu überzeugen.

In Deutschland sieht das ULD eine Pflicht zum Nachweis der Informationspflicht (beispielsweise durch ein Häkchen in der Software einer Arztpraxis für einen jeden Patienten)…. wenn sich diese Auffassung durchsetzen sollte, dann wird es sehr aufwändig.

e) Diverse Aspekte zur Auskunftspflicht

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite Fehler! Textmarke nicht definiert.).

Die Artikel-29-Datenschutzgruppe (siehe Seite 423) hat im Workingpaper „WP 260“ im April 2018 sehr ausführlich Stellung genommen zu allen Fragen der Auskunftspflicht bezüglich Artikel 13 und Artikel 14. Die vielfältigen Auswirkungen lassen sich kaum zusammenfassen (daher sollte man das 40-seitige englische Original besser selbst lesen). Nur so viel:

- Eine Publikation der Auskunftstexte im Internet wird explizit empfohlen (dort Seite 5)
- Wesentliche Änderungen an den Auskünften sollten den betroffenen Personen aktiv zugetragen werden (dort Seiten 5, 16, 17)
- Wesentliche Änderungen an der Datenverarbeitung sollten frühzeitig kommuniziert und beauskunftet werden, damit die betroffenen Personen schon vorab überlegen können, ob sie z.B. widersprechen oder Einwilligungen widerrufen wollen. Das gewählte Zeitfenster ist zu begründen (dort Seiten 17, 18, 24).
- Auch wenn sich Auskunftstexte nicht ändern, so könne es nicht schaden, wenn man die Texte immer wieder mal in Erinnerung ruft („express reminders“, dort Seite 18).
- Die Auskunftstexte sollten übersichtlich formatiert und mit einzelnen Überschriften versehen werden, um einer „Informations-Ermüdung“ vorzubeugen (dort Seite 7, 19)
- Auf Websites wird ein Link auf die Datenschutz-Unterrichtung erwartet, der mit maximal 2 Mausklicks erreichbar ist. Bei Online-Formularen sollte er sofort verlinkt werden (dort Seite 8).
- Die Auskunftstexte sollten in allen Sprachen verfügbar sein, die die typischen Leser erwarten würden (dort Seite 10).
- Die Auskünfte müssen gemeinsam in EINEM Dokument enthalten sein und dürfen somit nicht auf verschiedene Stellen verteilt werden (dort Seite 11).
- Die betroffenen Personen sollten die Auskünfte im Internet z.B. auch über QR-Codes zugreifen können (dort Seiten 12, 18).
- Ein „Privacy-Dashboard“ wird empfohlen, um die Auskünfte und Datenschutz-Einstellungen an EINEM Ort vornehmen zu können (dort Seite 20).
- Die Auskünfte können auch Angaben zu anderen Pflichten enthalten und insofern über die Artikel 13 und Artikel 14 hinausgehen (dort auf Seite 22). Im Rahmen des PrivazyPlan® wird bereits vorgeschlagen, dass sämtliche (!) Auskünfte in einem gemeinsamen Transparenztext zusammengefasst werden (siehe Seite 98).
  Im „WP 260“ auf den Seiten 22 und 36 geht man aber auf andere Sachverhalte ein: Beispielsweise
  - die Ergebnisse von Datenschutz-Folgenabschätzungen (siehe Pflicht **[GVO_035]** auf Seite 156) oder
  - zur Interessenabwägung (Seite 352) oder
  - zu Maßnahmen zur Datensparsamkeit (siehe Pflicht **[GVO_025]** auf Seite 93) oder
  - zu gemeinsam Verantwortlichen (siehe Pflicht **[GVO_026]** auf Seite 165).
- Falls eine Zweckänderung vorliegt, so sollte die Begründung der „Zweck-Kompatibilität“ geliefert werden (dort Seite 24). Dies zielt ab auf die Pflicht **[GVO_013a]** auf Seite 37.
- An keiner Stelle wird beschrieben, dass man die erteilten Auskünfte personenbezogen dokumentieren müsste. Allein auf Seite 27 wird dies thematisiert in Bezug auf die Frage, ob einer betroffenen Person nicht **noch einmal** eine Auskunft geliefert werden muss.
- Falls die Daten bei Dritten erhoben wurden (siehe Pflicht **[GVO_014]** auf Seite 41), so muss der Verantwortliche jederzeit nachweisen können, woher die Daten ursprünglich stammten. Auch Jahre später. Auch nach Portierungen in neue Datenbanken. Das ist eine weitgehende Forderung hinsichtlich der Software-Konzeption (siehe dort Seite 29).
- !!! Die Beauskunftung der externen Daten-Empfänger sollte explizit deren Namen erhalten, damit die betroffenen Personen erkennen können, wer alles auf die Daten zugreifen kann (dort Seite 37). Im Sinne der geforderten Fairness sollte man also die Namen der Firmen veröffentlichen, die als Auftragsverarbeiter oder Übermittlungs-Empfänger zu erwarten sind. Falls die Empfänger in Drittländern niedergelassen sind, so sollte das Land und die konkrete „Garantie“ genannt werden (dort Seite 37, 38).
- Die Löschfristen müssen konkret (und ggf. speziell für die jeweilige Datenkategorie) genannt werden. Auch Archivierungspflichten müssen genannt werden (siehe dort Seite 38, 39).

- In Formularen muss klar gekennzeichnet werden, welche Datenfelder notwendigerweise ausgefüllt werden müssen, und was die Konsequenzen sind, wenn die betroffene Person die Felder nicht ausfüllt (dort Seite 40).

Muss man die **konkreten Kontaktdaten der zuständigen Aufsichtsbehörde** nennen, um die Informationspflichten gemäß Artikel 13 (2d), Artikel 14 (2e) und Artikel 15 (1f) zu erfüllen? Der Wortlaut selbst lässt dies offen. Ein Blick in die Fachliteratur zeigt kontroverse Ansichten; zum Artikel 13 bejahen dies Gierschmann in RdNr. 105 und Kühling/Buchner in Rdnr. 39; hingegen lehnt es Gola in Rdnr. 22 ab. Um Beschwerden und Abmahnungen zu entgehen ist wohl die Nennung der Aufsichtsbehörden-Kontaktdaten empfehlenswert.

In Bezug auf **Direktwerbung** (per Post, E-Mail und Telefon) gilt: Dieser Verarbeitungszweck sollte unbedingt auch in der Zweckbeschreibung erwähnt werden. Denn wenn der Informationstext explizit auch den Zweck der Direktwerbung erwähnt, dann fällt später eine mögliche Interessenabwägung im Rahmen der „berechtigten Interessen“ gemäß Artikel 6 (1f) leichter (siehe Seite 352). Dies ergibt sich aus Satz 1 im Erwägungsgrund 47, wo die „vernünftigen Erwartungen“ der betroffenen Personen thematisiert sind.

2.1.3 Wie erfüllt man diese Pflicht [GVO_013] ?

Im Rahmen des PrivazyPlan® wird die unten folgende Vorgehensweise vorgeschlagen; dort wird für jede Phase des „plan-do-check-act“-Zyklus ein separates Dokument erstellt.

In aller Kürze geht es darum: ● Besorgen Sie sich das Verarbeitungsverzeichnis, um alle betroffenen Verarbeitungen zu identifizieren. ● Erstellen Sie den geforderten Informationstext (sofern er nicht schon durch einen gemeinsamen „Transparenz“-Text erstellt wurde, siehe Seite 324). ● Stellen Sie die Texte den betroffenen Personen in geeigneter Form zur Verfügung (z.B. auf der Website). ● Alle neuen/veränderten Verarbeitungen müssen unverzüglich erstellt und publiziert werden.

Selbstverständlich können Sie all diese Punkte auf Ihre speziellen betrieblichen Belange anpassen.

a) Planung einer Strategie („plan“)

Die Geschäftsleitung sollte sich zunächst eine ganz grundlegende Strategie überlegen. Im Folgenden liefern wir dafür eine Reihe von Anhaltspunkten. Erst danach sollte die Durchführung begonnen werden (siehe weiter unten). Sie können folgendermaßen vorgehen:

☐ Beachten Sie die allgemeinen Planungs-Hinweise auf Seite 21.

☐ Es ist nicht klar geregelt, ob der **Name des Datenschutzbeauftragten** in den Informationstexten explizit genannt werden muss. Die Geschäftsleitung sollte entscheiden, ob ein abstrakte E-Mail Adresse (wie z.B. datenschutz@meinUnternehmen.com oder privacy@myCompany.com) genannt werden soll, oder ob der Datenschutzbeauftragte namentlich genannt werden soll (z.B. „Sie erreichen Herrn Vollmer unter N.Vollmer@SecureDataService.de“).

☐ Es kann **Ausnahmen** geben. Der Erwägungsgrund 62 besagt, dass sich die Pflicht zur Information erübrigt, wenn **(a)** die betroffene Person die Information bereits hat, oder **(b)** wenn die Speicherung oder Offenlegung der Daten ausdrücklich durch Rechtsvorschriften geregelt ist, oder **(c)** wenn die Unterrichtung unmöglich ist oder mit einem unverhältnismäßig hohen Aufwand verbunden ist.
Diese Ausnahmen gilt es seitens der Geschäftsleitung ganz prinzipiell zu prüfen und zu diskutieren. Was bezweckt Brüssel mit diesen Ausnahmen? Gibt es offensichtliche Szenarien dieser Art? Wann kann sich das Unternehmen eine Information sparen, ohne dass es sich (vielleicht auch aufgrund eines Missverständnisses) möglicherweise einer Gefahr von Geldbußen aussetzt?
Falls das Unternehmen auf eine Information verzichtet: Wo sind die Gründe dafür dokumentiert? Hat die Geschäftsleitung diese Entscheidung explizit genehmigt?

☐ Spielen Sie alle Szenarien durch, wo Sie personenbezogene Daten erheben könnten. Relevant sind wohl insbesondere diese Wege: **Telefon,** E-Mail, Fax, eigene Website, Webinar-Software, Socialmedia (XING, facebook, …), Briefpost und im persönlichen Gespräch (z.B. auf einer Messe).

☐ Wenn die erhobenen Daten (z.B. auf einer Webseite) gespeichert werden: Wird dann ebenfalls dokumentiert, welcher konkreter Informationstext der betroffenen Person vorlag? Es würde reichen das entsprechende Kürzel (z.B. „i001_de“) zu speichern. Somit ließe sich im Nachhinein beweisen, dass (und wie) die Person informiert wurde.

☐ Was kann man tun, wenn z.B. wegen **Platzmangel** keine vorherige Information stattfinden kann? Dies ist beispielsweise zutreffend beim Automatenverkauf, bei Telefon-Geschäften und bei Gewinnspiel-Postkarten. In diesen Fällen wird es sehr schwierig sein, die geforderten Informationen zu liefern. Hier muss eine Entscheidung getroffen werden. Sollen beispielsweise **QR-Codes** angeboten werden, mit denen die Person per Smartphone schnell an die konkreten Informationstexte im Internet gelangen kann? Weitere Beispiele finden sich in der GDD-Praxishilfe DS-GVO VII auf Seite 9.

☐ Die (Informations-) Texte gemäß den Pflichten **[GVO_013]**, **[GVO_013a]**, **[GVO_014]**, **[GVO_015]** und **[GVO_030]** sind in weiten Teilen identisch. Es ist denkbar diese Texte in EINEM Dokument zusammenzufassen. Dies spart Zeit und verhindert Wiederholungen (siehe Seite 98). Wollen Sie diesen Weg gehen? ➔ Auf Seite 324 finden Sie ein Beispiel für diese Art der vereinheitlichten Dokumentation.

b) Durchführung („do“)

Wenn die obigen Planungen abgeschlossen sind, so kann diese Pflicht konkret bearbeitet werden. Es bedarf vorbereitender Maßnahmen, bevor diese Pflicht durchgeführt werden kann:

☐ Besorgen Sie sich das Verarbeitungsverzeichnis (gemäß Artikel 30 und der Pflicht **[GVO_030]** auf Seite 97). Die Liste liegt entweder bei Ihrem Datenschutzbeauftragten oder bei einer anderen dafür zuständigen Person. Anhand dieser Liste sehen Sie, worauf sich die zu erstellenden Informationstexte beziehen sollen.
(Eventuell könnte aus dem Verarbeitungsverzeichnis heraus ein passender Text erzeugt werden).

Und dann gilt für den Informationstext einer jeden einzelnen Verarbeitung:

☐ Formulieren Sie den Informationstext. Falls Sie keinen gemeinsamen Transparenztext für die Pflichten **[GVO_013]**, **[GVO_013a]**, **[GVO_014]**, **[GVO_015]** und **[GVO_030]** erstellen wollen, so können Sie den Text z.B. im Mini-Datenschutz-Managementsystem im Unterordner \GVO_013 ablegen (siehe Seite 26); andernfalls können Sie im Unterordner \GVO_030 einen gemeinsamen Text ablegen. Gemäß Erwägungsgrund 39 muss er leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst werden.

☐ Finden Sie heraus, an welchen Stellen die Daten bei den betroffenen Personen erhoben werden. Geschieht dies online und/oder per Fax oder auf Papier? Genau dort müssen später die Informationstexte publiziert werden. Dies kann sein: (a) auf der Webseite in direkter Nähe zum Eingabe-Formular, oder (b) auf Papier-Formularen z.B. in einem Anhang, oder (c) per Telefon, wo ein vorbereiteter Text verlesen wird.
Dokumentieren Sie im obigen Dokument, wann Sie den Text an welcher Stelle publiziert haben.
Falls Sie die „**gemeinsamen Transparenztexte**“ erstellt haben (siehe Seite 98) und im Internet publiziert haben (siehe http://www.securedataservice.de/transparenz), so können Sie in den Formularen etc. auf den jeweiligen Transparenztext verweisen (beispielweise per QR-Code).

☐ Besteht für diese Verarbeitung eine **gemeinsame Verantwortlichkeit** gemäß der Pflicht **[GVO_026]**, wie auf Seite 165 beschrieben? Dann muss den betroffenen Personen der wesentliche Inhalt der zugrundeliegenden Verträge zur Verfügung gestellt werden (siehe Seite 170). Der Anknüpfungspunkt ist Artikel 13 (1a), wo der Verantwortliche genannt werden muss: Hier würde man alle Verantwortliche aufzählen (und die wesentlichen Vertragsklauseln nennen).

Sie haben für alle Verarbeitungen einen Informationstext erstellt und publiziert? Dann ist die Phase der „Durchführung“ erst einmal abgeschlossen. Glückwunsch, Sie haben‘s geschafft!

c) Prüfung („check“)

Die Erfüllung dieser Pflicht muss ab dem 25.05.2018 wiederkehrend überwacht werden. Die für die Prüfung zuständige Person kann folgendermaßen vorgehen:

☐ Beachten Sie die allgemeinen Check-Hinweise auf Seite 23.

☐ Überlegen Sie sich eine relevante Prüffrage. Es gibt natürlich sehr viele verschiedene Aspekte zur Informationspflicht, die Sie erfragen könnten. Die folgenden Beispiele verdeutlichen dies:
• Gibt es Leitlinien oder Leitfäden im Umgang mit der Informationspflicht? Wie wird sichergestellt, dass das Unternehmen diese Pflicht konkret lebt?
• Nutzt das Unternehmen die Möglichkeiten der DS-GVO hinsichtlich der Tatbestände, wo die Information sich erübrigt? Wird das nachvollziehbar begründet?

• Verfügt das Unternehmen über eine Liste aller Informationstexte, um deren Vollständigkeit und Richtigkeit gezielt prüfen zu können?
• Wie stellt das Unternehmen sicher, dass die Informationstexte nicht von den Inhalten des Verarbeitungsverzeichnisses abweichen?
• Wie stellt das Unternehmen sicher, dass die Texte den betroffenen Personen verständlich sind und dass sie in den notwendigen Landessprachen vorliegen?
• Wie können Sie nachweisen, welche Informationstexte den betroffenen Personen zum Zeitpunkt der Datenerhebung vorlagen?

d) Verbesserungspotential mitteilen („act“)

Wenn die Überwachung der Pflicht über Verbesserungspotential verfügt, so muss dies formuliert und gemeldet werden.

☐ Beachten Sie die allgemeinen Act-Hinweise auf Seite 23.

In dieser Demo-Version werden die anderen Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version werden die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version werden die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Dieses Kapitel ist in Ihrer Version nicht enthalten.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

In dieser Demo-Version sind die Unterkapitel ausgeblendet.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Dieses Kapitel ist in Ihrer Version nicht enthalten.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Dieses Kapitel ist in Ihrer Version nicht enthalten.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Dieses Kapitel ist in Ihrer Version nicht enthalten.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 451; eine tabellarische Übersicht auf Seite 467.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 260.

Hier im Anhang befinden sich verschiedene Ansätze, um Ihnen den Überblick über die Pflichten zu erleichtern.

Sämtliche Texte des Anhangs liefern letztlich keine neuen Inhalte, sondern liefern Ihnen lediglich eine komprimierte Ansicht.

Ganz bewusst sind diese Seiten im Hochformat gestaltet und mit einem etwas breiteren Rand auf der linken Seite versehen. Somit können Sie diese Seiten bequem ausdrucken und abheften.

14.1 Kurzzusammenfassung aller Pflichten

Anhang

In den Kapiteln 2 bis 10 (auf den Seiten 29 bis 228) werden alle Pflichten des Verantwortlichen ausführlich beschrieben und angeleitet. Ein Klick auf den jeweiligen Absatz führt direkt nach oben in die Pflicht-Kapitel.

14.1.1 Pflichten aufgrund von Persönlichkeitsrechten

Die „*Rechte der betroffenen Personen*“ befinden sich im Kapitel III der DS-GVO in den Artikeln 12-23. Aus jedem Artikel ergeben sich eine oder mehrere Pflichten:

Bei Erhebung von Daten ausführlich informieren [GVO_013]

Gemäß Artikel 13 (1) und Artikel 13 (2) muss das Unternehmen die betroffenen Personen schon bei der Datenerhebung sehr ausführlich informieren. Dies soll die Fairness und Transparenz der Verarbeitung sicherstellen. Man könnte diese Information als eine Art „Beipackzettel“ ansehen.

➔ Die Pflicht **[GVO_013]** wird auf Seite 30 erklärt.

In aller Kürze geht es darum: ● Besorgen Sie sich das Verarbeitungsverzeichnis, um alle betroffenen Verarbeitungen zu identifizieren. ● Erstellen Sie den geforderten Informationstext (sofern er nicht schon durch einen gemeinsamen „Transparenz“-Text erstellt wurde, siehe Seite 324). ● Stellen Sie die Texte den betroffenen Personen in geeigneter Form zur Verfügung (z.B. auf der Website). ● Alle neuen/veränderten Verarbeitungen müssen unverzüglich erstellt und publiziert werden.

In dieser Demo-Version werden die anderen Pflichten ausgeblendet.

14.2 Ausführliches Inhaltsverzeichnis

Anhang

Auf Seite 2 findet sich aus Platzgründen nur ein grobes Inhaltsverzeichnis.
Für eine bessere Übersicht soll hier nun ein ausführliches Inhaltsverzeichnis nachgereicht werden.
Es kann durchaus hilfreich sein, dieses Inhaltsverzeichnis auszudrucken (siehe Seite 10).

14.3 Pflichten in tabellarischer Form

Anhang

Für einen besseren Überblick können Sie sich diese Seite ausdrucken (weitere Tipps für einen guten Überblick gibt es auf Seite 10).

Pflichten aufgrund von Persönlichkeitsrechten

Im Kapitel 2 werden alle „typischen“ Persönlichkeitsrechte erklärt:

2.1	Bei Erhebung von Daten ausführlich informieren [GVO_013]	Artikel 13 (1,2)	31
2.2			37
2.3			41
2.4			46
2.5			49
2.6			55
2.7			57
2.8			60
2.9			63
2.10			66
2.11			70
2.12			74
2.13			78
2.14			82

Pflichten zu Dokumentationen und Nachweisen

Im Kapitel 3 geht es um den allgemeinen „Dokumentationsaufwand“:

3.1	Nachweis der Einhaltung der „Grundsätze“ [GVO_005]	Artikel 5 (2)	87
3.2			93
3.3			97
3.4			102

Pflichten zu Rechtmäßigkeit und Einwilligung

Im Kapitel 4 wird die Rechtmäßigkeit (inkl. zahlreicher Einwilligungs-Aspekten) erklärt:

4.1	Datenverarbeitungen brauchen eine Rechtsgrundlage [GVO_006]	Artikel 6 (1)	108
4.2			116
4.3			121
4.4			125
4.5			127
4.6			130
4.7			134

Pflichten zu Sicherheit und Datenschutzverletzungen

Im Kapitel 5 wird die Informationssicherheit erläutert und Datenschutzverletzungen behandelt:

5.1	Informations-Sicherheits-Managementsystem einrichten [GVO_032]	Artikel 32 (1)	137
5.2			141
5.3			145
5.4			148
5.5			152

Pflichten zur Datenschutz-Folgenabschätzung und Konsultation

Im Kapitel 6 werden die Folgen eine Datenverarbeitung abgeschätzt und ggf. die Aufsichtsbehörde einbezogen:

6.1	Datenschutz-Folgenabschätzung [GVO_035]	Artikel 35	156
6.2			162

Pflichten in Hinblick auf andere Verantwortliche

Im Kapitel 7 dreht sich alles um verschiedene Formen des „Outsourcings“:

7.1	Gemeinsame Verantwortlichkeit [GVO_026]	Artikel 26	165
7.2			173
7.3			176
7.4			182
7.5			188
7.6			190

Pflichten zur Benennung eines Datenschutzbeauftragten etc.

Im Kapitel 8 wird die betriebliche Einbindung des Datenschutzbeauftragten (DSB) beschrieben und seine Aufgaben erläutert:

8.1	Benennung eines Datenschutzbeauftragten [GVO_037]	Artikel 37 (1)	195
8.2			201
8.3			204
8.4			207
8.5			209
8.6			211
8.7			214
8.8			217

Pflichten aus sonstigen Datenschutzvorschriften

Im Kapitel 9 geht es um datenschutzrelevante Vorschriften aus anderen Gesetzen. Die hier genannten Beispiele können für Unternehmen in Deutschland relevant sein:

9.4.3	a) Berufliche Schweigepflicht [STGB_203]	§ 203 StGB	224
9.4.3	b) Unzumutbare Werbe-Belästigungen [UWG_007]	§ 7 UWG	225

Pflichten durch das neue Bundesdatenschutzgesetz

Im Kapitel 10 geht es um datenschutzrelevante Vorschriften, die der deutsche Gesetzgeber aufgrund der Öffnungsklauseln nutzt. Die hier genannten Pflichten sind speziell für Unternehmen in Deutschland relevant:

~~10.1~~	~~OBSOLET: Videoüberwachungen kenntlich machen~~	~~§ 4 Abs. 2~~	~~231~~
~~10.2~~	~~OBSOLET: Identifizierte Personen von Videoüberwachung informieren [BDSG_004a]~~	~~§ 4 Abs. 4~~	~~232~~
10.3	Sicherheitsmaßnahmen bei sensiblen Daten [BDSG_022]	§ 22 Abs. 2	234
10.4			236
10.5			238
10.6			239
10.7			241
10.8			243

14.4 Unsichere Sachverhalte (rote Bomben)

Anhang

Bezüglich des EU-weiten Datenschutzes ab dem 25.05.2018 gibt es viele offene Fragen. Einige davon sind im PrivazyPlan® durch kleine rote Bömbchen ( ) gekennzeichnet (siehe Seite 8).

Sämtliche Bömbchen fassen wir hier nochmal konzentriert zusammen. Bitte klicken Sie auf den jeweiligen Text, um den Kontext besser zu verstehen.

14.4.1 Pflichten aufgrund von Persönlichkeitsrechten (Kapitel 2)

In dieser Demo-Version sind die Roten Bömbchen ausgeblendet.

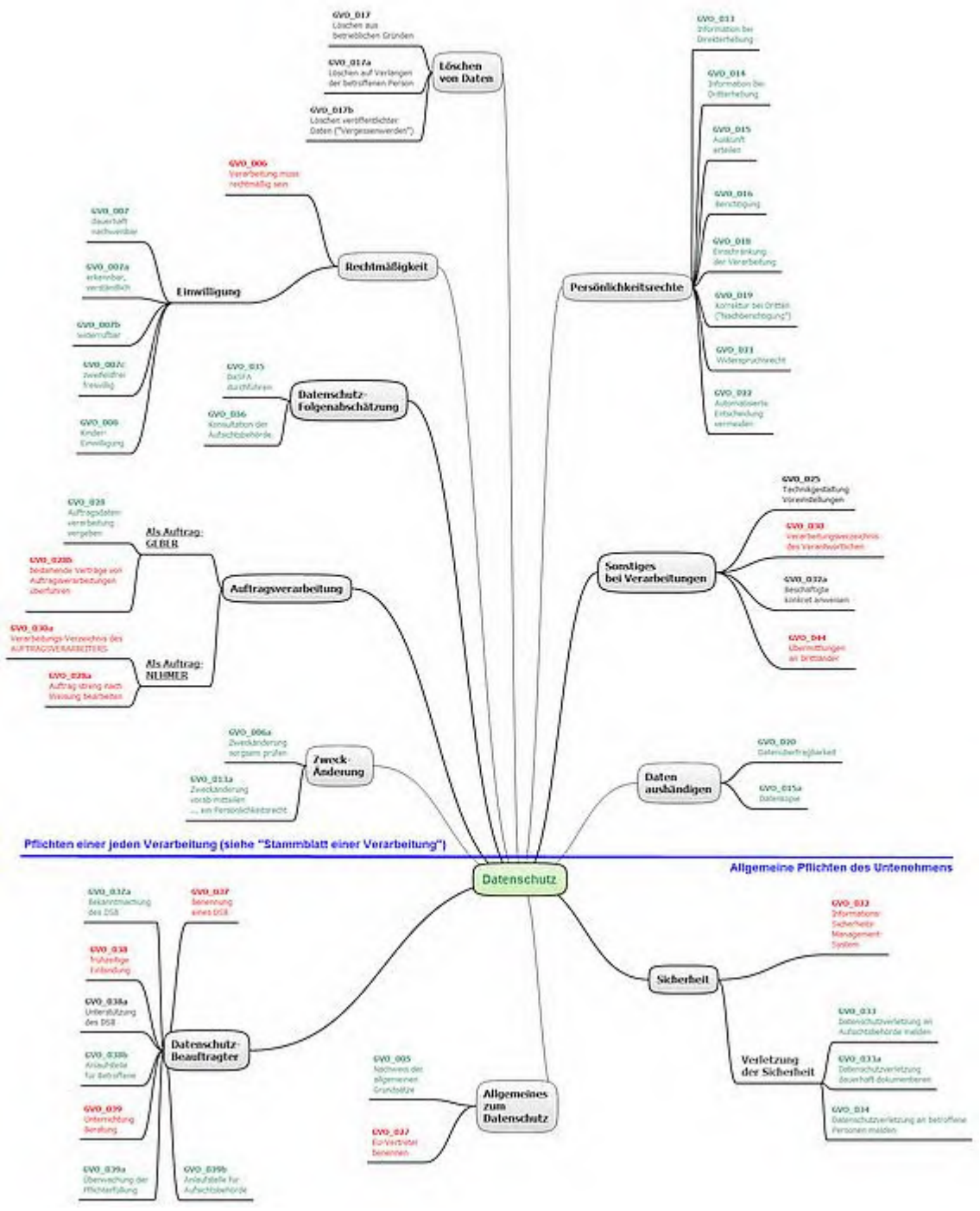
14.5 Mindmap der Pflichten

Anhang

Das folgende Mindmap zeigt die Pflichten im Sinne des Kapitels „Ausrichtung nach Pflichten (Schritt 3)“ auf Seite 11.

Alle Pflichten der DS-GVO sind enthalten (die Pflichten des BDSG sind aus Gründen der Übersichtlichkeit ausgespart). Die Pflichten oberhalb der blauen Linie betreffen jede einzelne Verarbeitung; die Pflichten darunter sind allgemeine Pflichten. Die roten Pflichten sollten sofort in Angriff genommen werden; die schwarzen Pflichten bis zum 25.05.2018; die grünen Pflichten sind erst nach dem 25.05.2018 relevant (müssen natürlich aber schon vorher vorbereitet werden).

Das Mindmap finden Sie in voller Qualität in der Datei **PrivazyPlan.zip** (siehe Seite 26) im Unterverzeichnis „_Allgemeines“.



Quelle: PrivazyPlanMindmap_demo.png

14.6 Index

Anhang

Die wichtigsten Begriffe werden hier im Index aufgeführt, um Ihnen die Suche zu erleichtern.

Aus technischen Gründen dienen die Seitenzahlen leider nicht als Hyperlinks direkt zur gewünschten Seite. Sie können manuell zur gewünschten Seite springen, indem Sie in Ihrem PDF-Reader die Tastenkombination „STRG+G“ drücken.

Im August 2017 ist dieser Index noch etwas rudimentär, aber dies wird sich im Laufe der monatlichen Updates ändern.

Beziehen sich die Begriffe auf das deutsche Bundesdatenschutzgesetz, so ist dies an einem angehängten „(DE)“ erkennbar.

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z