PRIVAZYPLAN®

Praxisleitfaden für Datenschutz.

PRIVAZYPLAN®
BRINGT IHREN DATENSCHUTZ
AUF KURS.

Alle Pflichten.
Alles erklärt.
Alles nach Plan.

von SecureDataService
Nicholas Vollmer

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

von
SecureDataService
Nicholas Vollmer

im Dezember 2017

Inhaltsverzeichnis

… ein ausführliches Inhaltsverzeichnis finden Sie auf Seite 374.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checkliste des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

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 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

1.1 Vorwort zur aktuellen Ausgabe

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen zur aktuellen Ausgabe im Dezember 2017. Was sind die wichtigsten Neuerungen in diesem Monat?

- **PrivazyPlan.xls: Gemeinsame Transparenztexte**
  Es hatte sich herausgestellt, dass es sinnvoll ist die verschiedenen Transparenztexte zu einem gemeinsamen Text zusammenzufassen (siehe Seite 91). Dies wird in einem neuen Tabellenblatt in der MS-Excel-Tabelle präzise dargestellt. Ganz am Ende der zahlreichen Tabellenblätter finden Sie diese Zusammenfassung. Den Hyperlink zur entsprechenden ZIP-Datei finden Sie auf Seite 26.

- **Neues Bömbchen: Keine Datenschutz-Folgenabschätzung bei Ärzten?**
  Der Erwägungsgrund 91 liefert Berufsgeheimnisträgern eine Ausnahme zur Datenschutz-Folgenabschätzung. Dementsprechend entfällt auch der diesbezügliche Grund zur Benennung eines Datenschutzbeauftragten. Kann ein Erwägungsgrund eine solch elementare Ausnahme begründen? Seite 143.

- **Kirchen in Deutschland haben neues Datenschutzrecht beschlossen**
  Die Evangelische und die Katholische Kirche in Deutschland haben im November ein neues Datenschutzrecht beschlossen, welches ab dem 25.05.2018 gilt und der DS-GVO stark ähnelt. Seite 202.

- **Auftragsverarbeitung bei Berufsgeheimnisträgern legalisiert (DE)**
  Jetzt endlich wurde der § 203 Strafgesetzbuch novelliert. Somit dürfen Ärzte, Rechtsanwälte etc. endlich ganz offiziell einen externen IT-Dienstleister oder Aktenvernichter beauftragen. Seite 204.

- **Grobe Checkliste für die ersten Schritte**
  Diese neue Checkliste ist der ultimative Startpunkt für den Verantwortlichen. Sie gibt der Geschäftsführung einen Überblick über die wichtigsten Entscheidungen und ersten konkreten Schritte. Von hier aus wird auf alle wichtigen Stellen im PrivazyPlan® verwiesen. Seite 233.

- **Interessenabwägung**
  An fast einem dutzend Stellen in der DS-GVO (und dem BDSG-neu) werden „überwiegende“ Interessen thematisiert. Dahinter verbirgt sich eine Interessenabwägung: Überwiegen die berechtigten Interessen des Verantwortlichen, oder die schützenswerten Interessen der betroffenen Personen? Dies ist leider ein sehr komplexes Thema, welches hier nur kurz angerissen werden kann. Seite 294.

- **Sachlicher Anwendungsbereich: Das Dateisystem**
  Gilt die DS-GVO auch bei personenbezogenen Daten auf Schmierzetteln? Wo ist denn die Grenze zu einem (nicht-) automatisierten Dateisystem? Dies ist eine wichtige Frage, weil sich daran die ca. 50 Pflichten des Verantwortlichen orientieren. Seite 356

In **6 Monaten** wird die EU-Datenschutz-Grundverordnung wirksam! Der **25. Mai 2018** rückt näher…

Ich wünsche Ihnen ein gutes Gelingen

N. Vollmer

P.S. Alle anderen 32 neue Stellen im PrivazyPlan® finden Sie, indem Sie nach dem Text „Neu im Dezember“ suchen.

1.2 Allgemeines Vorwort

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen.

Bitte erlauben Sie mir hier vorab einige einleitende - und persönliche - 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. Seit dem 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.

Für viele Datenschutzbeauftragte (auch für mich) war dies ein **„Schock“**. Wir hatten uns mit dem deutschen Bundesdatenschutzgesetz (BDSG) gemütlich gemacht, und niemand hätte je gedacht, dass es einmal eingestampft werden könnte. Nach 12 Jahren als hauptberuflicher Datenschutzbeauftragter wird es nochmal richtig spannend.

Schon im Juni 2016 stellte ich die Website www.privacy-regulation.eu fertig, um mir selbst (und meinen Kunden) überhaupt mal den reinen Verordnungstext zugänglich zu machen. Das hat sich als sehr hilfreich herausgestellt.

Eine echte **fachliche Beschäftigung** war im Grunde genommen erst möglich, als der erste Fachkommentar im November 2016 auf den Markt kam (siehe hier). Ab diesem Zeitpunkt fanden sich auch die ersten detaillierten Fachartikel in Fachzeitschriften.

Für deutsche Rechtsanwender war der zweite „Schock“ das stark **überarbeitete Bundesdatenschutzgesetz** (BDSG-neu) im April 2017. Auch hier war nach endlosen Diskussionen zunächst kein Ergebnis zu erwarten. Doch in einer Nacht-und-Nebel-Aktion war uns das neue BDSG beschert. Siehe www.bdsg2018.de. Also wurde alles noch komplizierter…

Im Ergebnis haben wir Datenschutzbeauftragte es nun mit zwei (sorry!) „zusammengeschusterten“ Bestimmungen zu tun, die in unnachahmlicher Komplexität nun einen Umfang von 85 statt früher 36 Seiten haben. Für die Umstellung haben unsere Kunden gerade mal ein Jahr Zeit.

Im Februar 2017 hatte ich begonnen die DS-GVO in ihre Pflichten zu zerlegen. Das war die Geburtsstunde des PrivazyPlan®. In den folgenden sechs Monaten wurden die ca. 50 Pflichten identifiziert, erklärt und angeleitet. Auf über 350 Seiten habe ich mein Bestes gegeben, um Ihnen einen praxistauglichen Leitfaden an die Hand zu geben.

Die nächsten zwei Jahre werden sehr spannend sein, denn es wird sich noch viel tun. Möglicherweise wird die ePrivacy-Verordnung noch bis zum 25.05.2018 in Kraft gesetzt (siehe Seite 201). Und hoffentlich werden uns die Aufsichtsbehörden noch mit klaren Checklisten und Vertragsvorlagen versorgen. Insofern gibt es für die monatlichen Updates des PrivazyPlan® garantiert viel Arbeit.

Den idealen Einstiegspunkt in die DS-GVO und den PrivazyPlan® erhalten Sie übrigens auf Seite 232.

Und nun, im August 2017, wünsche ich Ihnen eine angenehme Lektüre und ein gutes Gelingen!

N. Vollmer

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 Mai: …“ und „ Zurück zum Vorwort “.
  - Kleine Änderungen werden komplett eingefärbt und sehen dann folgendermaßen aus: „Neu im Mai: 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 330 Seiten Umfang ein recht großes Dokument. Wie können Sie da noch den Überblick behalten? Hierzu haben wir folgende Tipps:

- 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 darauf klicken 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-Rea-

der 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 354).

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 205 beschrieben werden. Weitere Details finden sich im Vorwort des Kapitels **10** auf Seite 206.

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 extrem 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 312). 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 drei mal 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 354). 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 Bußgelder, 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 daran halten.

- 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 312 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 380. 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 302 (mit einer Kurzzusammenfassung auf Seite 309).

Den idealen Einstiegspunkt in die DS-GVO und den PrivazyPlan® erhalten Sie übrigens auf Seite 232.

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 266
- die Kurzzusammenfassung aller Pflichten ab Seite 360
- das ausführliche Inhaltsverzeichnis ab Seite 374
- die tabellarische Übersicht aller Pflichten ab Seite 377
- den Index ab Seite 385

… 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.

➔ 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 http://www.privacy-regulation.eu. 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: Dossier „Datenschutzbeauftragte“. An vielen Stellen im PrivazyPlan® weisen wir auf diese Dossiers hin.

b) Das neue Bundesdatenschutzgesetz (BDSG-neu)

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 Paragraphen für die Privatwirtschaft.

➔ Unter www.bdsg2018.de/bdsg-neu-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 **Bußgelder vermeiden** (siehe Seite 339). 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 **bußgeldrelevanten 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 339 finden Sie weitergehende Informationen zu Bußgeldern, 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.“

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

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

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 Dossier „Nachweis" 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, und ein „TMG" für das Telemediengesetz.

- Der **hintere Teil** des Kürzels bezieht sich auf die Artikelnummer (bzw. ggf. den Paragraphen). Sollte ein Artikel oder Paragraph 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. Paragraphen-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 Bußgeldern drohen natürlich auch Schadenersatzforderungen. Die betroffenen Personen können gemäß Artikel 82 sowohl materielle als auch immaterielle Schäden geltend machen.
Doch lassen sich potentielle Schadenersatzforderungen im Verordnungstext noch schwieriger eingrenzen als Bußgeldgefahren. 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 Bußgeldgefahren.

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 Bußgeldbestimmung zu finden ist (siehe auch Seite 339),
- 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.

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

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

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 312).

Für wichtige Themen bieten wir auch noch **detaillierte Fachinformationen im** Kapitel 13 ab Seite 298. 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 302), 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 20.
- **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 230. 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 221-230).

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-neu 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 178.

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

Einleitung

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 235).

1.5.1 Welches Compliance-Managementsystem passt zu Ihnen?

Bekanntlich ist der Datenschutz ein **Compliance**-Thema (siehe Seite 302).

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?

Wie „hoch“ soll Compliance also aufgehängt werden? Wie „professionell“ soll das Ergebnis sein? Jedes Unternehmen muss hier eine Lösung finden, die zu ihm passt. Erläuternde Überlegungen finden Sie im Kapitel „Compliance“ auf Seite 302.

Auf welchem Weg soll z.B. der Datenschutzbeauftragte die Pflichterfüllung im Sinne des Artikel 37 überwachen? Wie soll also der (lesende) Zugriff auf die Dokumente und Nachweise ermöglicht werden? Es gibt verschiedene Möglichkeiten, wie beispielsweise: **(a)** durch Datenaustausch per E-Mail oder **(b)** durch Zugriff des Datenschutzbeauftragten per Remotedesktop bzw. VM-Ware auf das Firmennetz, oder **(c)** mittels Zugriff auf einen im Internet gehosteten Sharepoint-Server?

➔ Im Rahmen der Datei „**PrivazyPlan.zip**“ stellen wir den Ansatz für ein Minimal-Datenschutz-Managementsystem zur Verfügung (siehe Seite 26).

1.5.2 Was tun mit Betriebsrat / Datenschutzbeauftragten / Betriebsarzt?

Auch in diesen „Unternehmensteilen“ werden personenbezogene Daten gespeichert und genutzt. Trotzdem war der konkrete Datenschutz in diesen Betriebsteilen für die Geschäftsleitung ein eher weißer Fleck auf der Datenschutz-Landkarte.

Insbesondere ist die Kontrolle der Datenschutzmaßnahmen im Betriebsrat bisher nur wenig thematisiert und kontrolliert worden (was nicht zuletzt auch durch einen deutschen Gerichtsbeschluss aus dem Jahr 1997 bedingt ist… dort wurde dem betrieblichen Datenschutzbeauftragten die Kontrolle des Betriebsrates versagt worden).
Die Datenverarbeitung des Betriebsrats und die Zusammenarbeit mit dem Datenschutzbeauftragten sind im Kapitel 3.11.4 des TOM-Guide® beschrieben.

Treffen Sie eine Entscheidung: Wie soll der Datenschutz ab dem 25.05.2018 im Rahmen der DS-GVO beim Betriebsrat / Datenschutzbeauftragten / Betriebsarzt aussehen? [3]

Angesichts der drohenden Bußgelder und (auch immateriellen) Schadenersatzforderungen (siehe Seite 339) sollte es im Rahmen der DS-GVO ab dem 25.05.2018 keine weißen Flecken mehr geben. Die Geschäftsleitung sollte entscheiden, wie damit umgegangen werden soll.

1.5.3 Unterliegen verschlüsselte Daten der DS-GVO?

Eine der Kardinalfragen im Datenschutz lautet: Unterliegen **verschlüsselte** Daten dem Datenschutz und somit den Bestimmungen der DS-GVO?

Diese zentral wichtige Fragestellung wird im Kapitel 13.9 auf Seite 335 erläutert.

Treffen Sie eine Entscheidung: Stimmen Sie zu, dass verschlüsselte Daten dem Datenschutz unterliegen?

In dem oben genannten Kapitel finden sich Hinweise, worauf sich diese Entscheidung auswirken kann. Dies sollte sich bei der Erledigung der ca. 50 Pflichten widerspiegeln.

1.5.4 Inwieweit unterliegen Papier-Unterlagen der DS-GVO?

Neu im Dezember:
Leider gibt es einen großen rechtlichen Graubereich in Hinblick auf unsystematische Papierunterlagen. Gilt hier in jeder Hinsicht die DS-GVO? Diese Sachfrage wird auf Seite 356 ausführlich erläutert.
Zurück zum Vorwort

1.5.5 Gemeinsame Transparenztexte

Neu im Dezember:
Die betroffenen Personen haben gemäß der DS-GVO an verschiedenen Stellen das Recht auf Information bzw. Transparenz. Hiervon sind verschiedene Pflichten betroffen.
Beispielsweise für die Verarbeitung des Website-Kontaktformulars müssten ca. fünf verschiedene Texte geschrieben werden, die sich aber in weiten Teilen stark ähneln.
Man könnte diese Texte für jede Verarbeitung zusammenfassen. Das würde Zeit und Nerven sparen. Die Details werden auf Seite 91 ausführlich erläutert. Möchten Sie diesen Ansatz wählen?
Zurück zum Vorwort

[3] Zumindest in Bezug auf den Betriebsrat stellt sich diese Frage auch die Fachzeitschrift ZD 07/2017 Seite 322.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

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.

Jede Pflicht beginnt auf einer neuen Seite, damit Sie 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. [4]

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 Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) gab es keine derartigen Pflichten. Allenfalls im § 13 Abs. 1 TMG gab es eine vergleichbare Pflicht in Hinsicht auf die Unterrichtungspflicht auf Webseiten (siehe Pflicht **[TMG_013]** auf Seite 203).

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente: ● DSK-Kurzpapier ● 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] ?

Im Vergleich zum § 34 Abs. 1 BDSG 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 60).
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.

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.

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 Bußgeldern oder Schadenersatzforderungen ist hoch.

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

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 274). ● 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 20.

☐ 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 Bußgeldgefahr aussetzt?
Falls das Unternehmen auf eine Information verzichtet: Wo sind die Gründe dafür dokumentiert? Hat die Geschäftsleitung diese Entscheidung explizit genehmigt?

☐ 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 91). Wollen Sie diesen Weg gehen? ➔ Auf Seite 274 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 90). Die Liste liegt entweder bei Ihrem Datenschutzbeauftragten oder bei einer anderen dafür zuständigen Person. An-

hand 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:

☐ 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.

☐ Besteht für diese Verarbeitung eine **gemeinsame Verantwortlichkeit** gemäß der Pflicht **[GVO_026]**, wie auf Seite 150 beschrieben? Dann muss den betroffenen Personen der wesentliche Inhalt der zugrundeliegenden Verträge zur Verfügung gestellt werden (siehe Seite 153). 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.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

3.0 Einleitung

Dokumentation und Nachweis

Diese Dokumentations- und Nachweispflichten sind besonders wichtig in Hinsicht auf die **Aufsichtsbehörden**. Im Falle von Kontrollen werden die Aufsichtsbehörden die hier beschriebenen Dokumente anfordern.

Sollte der Verantwortliche nicht „liefern“ können, so führt dies zwangsläufig zu Problemen. Im Extremfall droht alleine schon deswegen ein Bußgeld.

Im Rahmen des PrivazyPlan® wird das Dossier „Nachweis“ angeboten. Dort werden die relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, dieses weitreichende Thema besser zu verstehen.

3.1 Nachweis der Einhaltung der „Grundsätze“ [GVO_005]

Dokumentation und Nachweis

Gemäß Artikel 5 (2) unterliegt der Verantwortliche einer generellen „*Rechenschaftspflicht*“. Inhaltlich basierend auf Artikel 5 (1) sind verschiedene Themenbereiche zu behandeln. Dabei ist insbesondere der Artikel 5 (1a) hervorzuheben, der ziemlich direkt ein Compliance-Managementsystem einfordert. Es ist zu erwarten, dass die Aufsichtsbehörden hier eine überzeugende Gesamtdokumentation anfordern.

Dieser Pflicht wird das Kürzel **[GVO_005]** zugeordnet (siehe Seite 12).

3.1.1 Allgemeine Informationen zur Pflicht [GVO_005]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (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 312) gibt es viele hilfreiche Dokumente: Die 16-seitige GDD-Praxishilfe DS-GVO IX („Accountability“) geht auf diese Pflicht ein.

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

3.1.2 Was bedeutet diese Pflicht [GVO_005] ?

Diese Pflicht ist zeitkritisch!
Um ein Chaos in der Dokumentation zu vermeiden, sollte die Geschäftsleitung ganz zu Anfang entscheiden, wie das Dokumentationssystem aufgebaut werden soll (eine grobe Priorisierung der Pflichten findet sich auf Seite 16).

Die „*Rechenschaftspflicht*“ gemäß Artikel 5 (2) führt dazu, dass sich das Unternehmen mit sechs wichtigen Themengebieten auseinandersetzen muss:

- Rechtmäßigkeit und Transparenz (siehe Seite 302 zum Thema „**Compliance**“)
- Zweckbindung
- Datenminimierung (siehe Seite 349)
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Diese hier vorliegende Rechenschaftspflicht hat natürlich große Schnittmengen mit den anderen ca. 50 Pflichten der DS-GVO. Davon sollte man sich nicht irritieren lassen. Möglicherweise wollte Brüssel mit dieser Rechenschaftspflicht verhindern, dass man „den Wald vor lauter Bäumen nicht sieht“. In diesem Sinne könnte diese Rechenschaftspflicht eine „Grundsatz-Strategie“ zum Ergebnis haben.

In dem Buch „Datenschutz“ von Jochen Schneider wird auf Seite 54 beschrieben, dass sich der Artikel 5 sehr stark an dem Artikel 8 der EU-Datenschutz-Richtlinie von 1995 orientiert; dort war die Überschrift „*Grundsätze in Bezug auf die **Qualität** der Daten*“). Insofern kann man durchaus sagen, dass der Artikel 5 die Qualität der Daten sicherstellen soll. Der Autor weist übrigens auf Seite 40 und 55 darauf hin, dass diese Vorschriften **viel zu unbestimmt sind**, als dass sich derart hohe Bußgelder (siehe Seite 339) begründen ließen (siehe Wikipedia).

Gola schreibt in RdNr. 33 zu Artikel 5:

> „*Die Rechenschaftspflicht führt damit in der Praxis im Vergleich zum bisherigen Recht zu **umfangreichen** zusätzlichen **Dokumentations- und Nachweispflichten**. Im Zweifel werden Unternehmen auf Nummer sicher gehen, und möglichst viele Dokumente produzieren, um nachzuweisen, dass sie in datenschutzrechtlicher Hinsicht compliant sind. Jedenfalls wird die Nachweispflicht künftig ein weites Tätigkeitsfeld in der Compliance-Beratung sein.*“

Kühling/Buchner schreiben in RdNr. 79f zu Artikel 5:

> „*Diese Nachweispflicht hat insbesondere Bedeutung im Hinblick auf Überprüfungen durch die Aufsichtsbehörden, die nach Art. 58 Abs. 1 lit. a auch die Befugnis haben, den Verantwortlichen zur Bereitstellung von Informationen anzuweisen. […] Empfehlenswert ist in jedem Fall eine schriftliche Dokumentation, aus der hervorgeht, in welcher Weise der Verantwortliche für die Einhaltung der Grundsätze des Artikel 5 Abs. 1 Sorge trägt*“.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

4.0 Einleitung

Rechtmäßigkeit und Einwilligung

Wann ist eine (Daten-) Verarbeitung zulässig? Oder wann greift sie zu sehr in die schützenswerten Rechte und Freiheiten der betroffenen Person ein?

Diese Fragestellung ist oftmals komplex. Und die DS-GVO liefert hierzu keine systematische Antwort. Vielmehr muss der Verantwortliche sich selbst überlegen, wie er die Rechtmäßigkeit korrekt prüft und nachweist.

Es gibt einen wichtigen Satz, den man sich immer wieder vor Augen führen muss:

> „Eine Verarbeitung ist zulässig, wenn
> (a) ein **Gesetz**, ein **Vertrag**, oder eine **Einwilligung** zugrunde liegt,
> (b) sie einem **Beschäftigungsverhältnis** dient,
> (c) der Verantwortliche ein berechtigtes und überwiegendes **Interesse** hat,
> (d) oder sonstige Rechtsgrundlagen bestehen, wie beispielsweise eine **Betriebsvereinbarung**."

Dieser obige Satz ist zwar eine grobe Vereinfachung der Sachlage, aber er hilft immer wieder die Orientierung zu wahren.

Warum ist dieser Satz eine grobe Vereinfachung? Dies soll hier kurz angerissen werden:

- Ein **Gesetz** muss diese Verarbeitung explizit **fordern**. Und es darf den Grundprinzipien der DS-GVO nicht widersprechen. Außerdem muss man prüfen, ob jenes Gesetz nicht vielleicht durch die DS-GVO „überschrieben" wird und somit nicht mehr anwendbar ist. Keine leichte Sache.

- Ein **Vertrag** muss mit der betroffenen Person abgeschlossen sein. Es mag aber auch vertragliche Ansprüche Dritter geben, die nur schwer einzuschätzen sind. Der Vertrag darf keine unverhältnismäßige Kopplung zu anderen Leitungen darstellen.

- Eine **Einwilligung** muss absolut freiwillig sein und kann jederzeit widerrufen werden. Sie muss dauerhaft nachweisbar sein. Bei Kindern gelten besondere Auflagen. Einwilligungen können verfallen, wenn sie längere Zeit nicht durch den Verantwortlichen genutzt werden.

- Beim **Beschäftigungsverhältnis** sind möglicherweise die jeweiligen gesetzlichen Bestimmungen des jeweiligen Landes zu beachten.
  In Deutschland ist dies der § 26 BDSG-neu.

- Das **berechtigte Interesse** des Verantwortlichen ist sorgsam abzuwägen. Er muss eine Interessenabwägung nachweisen können (siehe Seite 294). Die betroffenen Personen können dem widersprechen.

- Eine **Betriebsvereinbarung** kann einen Drahtseiltanz bedeuten, wenn man eine bestimmte Verarbeitung legitimieren möchte ohne das Schutzniveau der DS-GVO zu unterschreiten.

- Bei besonders „sensiblen" personenbezogenen Daten gelten separate Regelungen in der DS-GVO.

All die obigen Punkte betreffen die Frage nach der generellen Rechtmäßigkeit einer Verarbeitung. Dies ist das Thema des hier vorliegenden Kapitels 4.

Hinzu kommen aber noch andere Aspekte der Rechtmäßigkeit. Insbesondere bei der Weitergabe von Daten an Dritte (innerhalb und außerhalb der EU/EWR) wird diese Frage nochmal aufkommen (siehe Pflicht **[GVO_044]** auf Seite 172).

4.1 Datenverarbeitungen brauchen eine Rechtsgrundlage [GVO_006]

Rechtmäßigkeit und Einwilligung

Der Verantwortliche darf personenbezogenen Daten nur verarbeiten, wenn es hierfür eine spezifische Rechtsgrundlage gibt. Typischerweise wäre dies eine gesetzliche Grundlage oder ein Vertrag oder eine Einwilligung. Die DS-GVO und das BDSG-neu bieten hier ca. 30 Möglichkeiten. Bei sensiblen Daten gelten besonders hohe Hürden.

Dieser Pflicht wird das Kürzel **[GVO_006]** zugeordnet (siehe Seite 12).

4.1.1 Allgemeine Informationen zur Pflicht [GVO_006]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) bestanden ähnliche Notwendigkeiten im Rahmen von § 4 BDSG („Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung“).
Der Düsseldorfer Kreis hat festgestellt, das bestehende Einwilligungen auch nach dem 25.05.2018 weiterhin gültig sind.

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente.

[Im Rahmen von PrivazyPlan® wird das Dossier „Erlaubnis“ (10 Treffer) und das Dossier „Einwilligung“ (33 Treffer) angeboten. Dort werden die relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, diese weitreichenden Themen besser zu verstehen.]

4.1.2 Was bedeutet diese Pflicht [GVO_006] ?

Jede Verarbeitung braucht eine konkrete rechtliche Grundlage (Gesetz, Vertrag, Einwilligung, berechtigte Geschäftsinteressen, etc.). Diese muss der Verantwortliche herausfinden. Leider gibt es recht viele Grenzfälle, sodass die korrekte Rechtsgrundlage nicht immer leicht zu finden ist.

a) Generell gilt das Verbot mit Erlaubnisvorbehalt

Im Datenschutz gilt der Grundsatz: „**Es ist verboten, was nicht explizit erlaubt wird**“. Diese Argumentation ist erstmal sehr ungewöhnlich, denn in der juristischen Denkweise sieht man dies meistens genau umgekehrt. [18]
So gesehen hat sich in der DS-GVO im Vergleich zum BDSG nichts geändert. Der Verantwortliche braucht eine konkrete Rechtsgrundlage, damit er personenbezogene Daten verarbeiten darf.

Die DS-GVO liefert **kein abgestimmtes Konzept** an Rechtsgrundlagen. Vielmehr stehen verschiedenste Rechtsgrundlagen zusammenhanglos nebeneinander und über die gesamte DS-GVO verteilt. Der Verantwortliche muss also zunächst alle potentiellen Rechtsgrundlagen identifizieren und dann für jede Verarbeitung die passende Rechtsgrundlage finden. Erschwerend kommt hinzu, dass nationale Gesetze die Komplexität erhöhen können.

In dem folgenden Unterkapitel liefern wir die Liste der ca. 30 möglichen Rechtsgrundlagen. Die Reihenfolge ist dabei nicht unerheblich. Bei der Suche nach einer Rechtsgrundlage sollte man die folgende Liste von oben nach unten durchsuchen. Leider ist dies kein trivialer Vorgang (auch im BDSG in der alten Fassung war dies schon ein Problem… und nun ist es noch komplexer geworden).

b) Rechtmäßigkeit bei „besonderen Kategorien“ personenbezogener Daten

Der Artikel 9 (1) definiert eine Reihe von personenbezogenen Daten als „besondere Kategorien“. Hier im PrivazyPlan® werden diese Daten öfter auch schon mal als „**sensible Daten**“ bezeichnet (auch wenn dies streng fachlich gesehen vielleicht keine besonders präzise Formulierung ist… sie liest sich aber einfach sehr viel besser [19]).

Hierunter fallen alle Daten,

1.) **zur rassischen und ethnischen Herkunft,**

[18] Die „normale“ juristische Denkweise lautet: „Erlaubt ist, was nicht verboten ist“.

[19] Außerdem nimmt die DS-GVO im Erwägungsgrund 10 eine ähnliche sprachliche Vereinfachung vor.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

5.1 Informations-Sicherheits-Managementsystem einrichten [GVO_032]

Sicherheit und Datenschutzverletzungen

Es sind technische und organisatorische Maßnahmen zu treffen, um eine sichere Datenverarbeitung gemäß Artikel 32 (1) dauerhaft sicherzustellen. Dabei muss das Risiko der jeweiligen Datenverarbeitung angemessen berücksichtigt werden. Nur ein „Informations-Sicherheits-Managementsystem“ (ISMS) kann all dies gewährleisten.

Dieser Pflicht wird das Kürzel **[GVO_032]** zugeordnet (siehe Seite 12).

5.1.1 Allgemeine Informationen zur Pflicht [GVO_032]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) gab es keine derartigen Pflichten. Zwar gab es die technisch-organisatorischen Maßnahmen gemäß § 9 BDSG, aber ein systematisches ISMS war nicht vorgeschrieben.

Im Bundesdatenschutzgesetz (in der neuen Fassung ab dem 25.05.2018) werden durch § 22 Abs. 2 Satz 2 BDSG-neu in Bezug auf „besondere Kategorien“ personenbezogener Daten zusätzliche Aspekte zur Sicherheit der Verarbeitung gefordert. Insbesondere im Gesundheits- und Sozialbereich ist dies zu beachten. Die Pflicht **[BDSG_022]** berücksichtigt dies; konkret sind hiervon insbesondere die Maßnahmen zu den Zugangs- und Eingabe-Kontrollen betroffen (siehe Seite 211 und 212).

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente.

5.1.2 Was bedeutet diese Pflicht [GVO_032] ?

⚠ Diese Pflicht ist zeitkritisch!

Wenn das Unternehmen die Informations-Sicherheit systematisch fördern will, so muss dies gründlich geplant und schnell ausgeführt werden (siehe Seite 316). Diese Pflicht sollte daher möglichst früh bearbeitet werden (eine grobe Priorisierung der Pflichten findet sich auf Seite 16.

a) Wie wird die IT-Sicherheit in Ihrem Hause bisher betrieben?

Ganz sicher strebt auch Ihr Unternehmen bereits heute ein gewisses Maß an IT-Sicherheit an. Doch ist die IT-Sicherheit vielleicht kein zentrales Ziel der Geschäftsleitung. Die Maßnahmen sind aber häufig eher punktuell als systematisch. Die Schwerpunkte werden eher subjektiv vergeben. Und die Überwachung dieser Maßnahmen findet unregelmäßig (wenn überhaupt) statt. Würde die IT-Sicherheit von einem externen Auditor geprüft, so würde das Unternehmen sofort durchfallen, weil es noch nicht einmal die geforderten Dokumente und Nachweise liefern könnte (geschweige denn die strengen Kriterien einzuhalten).

Ja, das ist wohl in vielen Unternehmen der Normalzustand. Und es hat ja (mehr oder weniger) auch funktioniert. Allerdings nehmen die Hacker-Angriffe beständig zu, und sie werden auch immer professioneller. Hinzu kommt, dass Computer-Schwachstellen von Geheimdiensten gekauft werden… die dann früher oder später auf den „Markt“ kommen und weltweit hunderttausende Computer schädigen.

Mittlerweile ahnen viele Geschäftsführer, dass das knappe Budget der IT-Abteilung zu einem Problem werden könnte. Doch gab es bisher keine Gesetze, die auf breiter Front von der gesamten Wirtschaft und Verwaltung eine systematische IT-Sicherheit gefordert hätte. Diesbezügliche Bußgelder und Schadenersatzforderungen waren nicht zu erwarten. Das ändert sich nun durch die EU Datenschutz-Grundverordnung!

b) Was verlangt die DS-GVO?

Hinsichtlich der „Sicherheit der Verarbeitung“ stellt der Artikel 30 (1) umfangreiche Forderungen auf. Jegliche Verstöße können gemäß Artikel 83 (4a) mit Bußgeldern bis zu 10 Mio. € geahndet werden (siehe Seite 339); außerdem sind Schadenersatzforderungen (auch für immaterielle Schäden) gemäß Artikel 82 möglich (siehe Seite 339).

Die folgenden Aspekte sind wichtig:

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

6.1 Datenschutz-Folgenabschätzung [GVO_035]

Datenschutz-Folgenabschätzung und Konsultation

Die Datenschutz-Folgenabschätzung gemäß Artikel 35 soll die Risiken für die Rechte und Freiheiten der betroffenen Personen analysieren und dann vorbeugend minimieren (ähnlich der datenschutzfreundlichen Technikgestaltung bzw. Voreinstellungen). Bei einem hohen Restrisiko muss gemäß Artikel 36 die Aufsichtsbehörde konsultiert werden.

Dieser Pflicht wird das Kürzel **[GVO_035]** zugeordnet (siehe Seite 12).

6.1.1 Allgemeine Informationen zur Pflicht [GVO_035]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) bestanden ähnliche Pflichten im Rahmen von § 4d Abs. 5 BDSG („Vorabkontrolle"), siehe Kapitel 3.4 im TOM-Guide®. Die Formalitäten waren nicht so umfangreich, wie hier in der DS-GVO.

Im Bundesdatenschutzgesetz (in der neuen Fassung ab dem 25.05.2018) wird durch § 38 Abs. 1 BDSG-neu die Benennung eines Datenschutzbeauftragten notwendig, sobald sich die Notwendigkeit einer Datenschutz-Folgenabschätzung ergibt. Dies betriff die Pflicht **[GVO_037]** auf Seite 177.

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente: ● Fachbuch „Privacy Impact Assessment" von Mathias Reinis für 25 € ● Sehr gute Erläuterungen finden sich in der Trainingseinheit 3 der Informationsreihe „Fit für die Datenschutz-Grundverordnung". ● Das Kurzpapier-18 der Bayerischen Aufsichtsbehörde ist lesenswert. ● Das Kurzpapier 5 der Datenschutzkonferenz ● Die Aufsichtsbehörde Rheinland-Pfalz veröffentlichte 2013 eine 11-seitige Handreichung. ● Der Bitkom-Verband veröffentlich im Mai 2017 einen 64-seitigen Leitfaden zum Risk-Assessment und zur Datenschutz-Folgenabschätzung ● das 48-seitige Whitepaper „Datenschutz-Folgenabschätzung" des „Forum Privatheit" vom Mai 2016.

[Im Rahmen von PrivazyPlan® wird das Dossier „Datenschutz-Folgenabschätzung" angeboten. Dort werden die relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, diese weitreichenden Themen besser zu verstehen.]

6.1.2 Was bedeutet diese Pflicht [GVO_035] ?

a) Was ist ein „Risiko"?

Bei der Datenschutz-Folgenabschätzung dreht sich alles um das Thema „Risiko". Leider bleibt die DS-GVO aber eine Definition und auch sonst jede Erläuterung schuldig.

In den unten folgenden Ausführungen wird einige Fachliteratur genannt. Übergreifend gesehen könnte die ISO 31000 zum Risikomanagement interessant sein (englisch, 134 €).

[Im Rahmen von PrivazyPlan® wird das Dossier „Risiko" angeboten. Dort werden die relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, diese weitreichenden Themen besser zu verstehen.]

b) Was ist eine Datenschutz-Folgenabschätzung?

Der Verantwortliche soll sich dem Risiko seiner Datenverarbeitungen bewusst werden. Er soll gezielte Sicherheitsmaßnahmen planen, um allen Risiko-Szenarien begegnen zu können.

Hierbei handelt es sich um eine ziemlich aufwändige Abschätzung. Es geht darum, dass Verarbeitungen mit erhöhtem Risiko für die Rechte und Freiheiten der betroffenen Personen besonders sorgfältig geplant werden.

Der Verantwortliche muss sich zunächst überlegen, inwieweit eine geplante Verarbeitung ganz konkret einen Schaden bei den betroffenen Personen verursachen könnte (materiell und immateriell). Anschließend plant der Verantwortliche für jedes einzelne Schadensszenario eine Reihe von Sicherheitsmaßnahmen.

Wenn die Sicherheitsmaßnahmen alle Schadenszenarien ausreichend schützen, so besteht kein hohes (Rest-) Risiko und die Verarbeitung darf durchgeführt werden. Andernfalls ist die Aufsichtsbehörde zu konsultieren.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

7.1 Gemeinsame Verantwortlichkeit [GVO_026]

Andere Verantwortliche

Die gemeinsame Verantwortlichkeit gemäß Artikel 26 soll es mehreren Unternehmen erlauben, eine Verarbeitung gemeinsam – und zu den jeweils eigenen Zwecken – durchzuführen. In Hinblick auf Bußgelder und Schadenersatzforderungen haften alle Verantwortlichen gemeinschaftlich. Ein ausführlicher Vertrag ist dringend angeraten (die wesentlichen Inhalte sind den betroffenen Personen zur Verfügung zu stellen). Auch ohne Vertrag – also durch faktische gemeinschaftliche Handlung – entsteht dieses rechtliche Gebilde.

➔ Ein Überblick über alle Arten der Datenweitergabe findet sich auf Seite 320.

Dieser Pflicht wird das Kürzel **[GVO_026]** zugeordnet (siehe Seite 12).

7.1.1 Allgemeine Informationen zur Pflicht [GVO_026]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) gab es keine derartigen Pflichten bzw. Möglichkeiten. Dies liegt daran, dass die EU-Richtlinie von 1995 nicht konsequent in deutsches Recht umgesetzt wurde. Allenfalls im § 6 Abs. 2 BDSG wird thematisiert, dass „mehrere Stellen speicherungsberechtigt“ sein können.

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente: ● Die Zeitschrift ZD berichtet in 11/2016 auf Seite 512-517 ● Der Bitkom-Verband veröffentlicht im Mai 2017 eine 5-seitige Checkliste zur gemeinschaftlichen Verantwortlichkeit. ● Ausführlich in der Zeitschrift DuD 11/2016 Seite 512-522. ● Die Artikel-29-Datenschutzgruppe hat am 16.02.2017 im Workingpaper „WP 169“ auf Seite 21-30 zahlreiche Beispiele aufgeführt (das bezieht sich auf die Datenschutz-Richtlinie von 1995).

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

7.1.2 Was bedeutet diese Pflicht [GVO_026] ?

a) Was ist eine gemeinsame Verantwortlichkeit?

Die Begriffsdefinition des „Verantwortlichen“ in Artikel 4 Nr. 7 beinhaltet ein wichtiges Detail:

> *„[Der Ausdruck] **Verantwortlicher** [bezeichnet] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein **oder gemeinsam mit anderen** über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“*

Dies greift der Artikel 26 auf und legt fest:

> *„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel einer Verarbeitung fest, so sind sie „**gemeinsam Verantwortliche**“* (engl. „Joint Control“).

Diese Konstruktion der gemeinsamen Verantwortlichkeit wurde schon im Jahr 1995 im Artikel 2 lit d. der Richtlinie 95/46/EG erwähnt (aber nicht weiter präzisiert). In Deutschland wurde dies im Jahr 2001 aber nicht in deutsches Recht übernommen (weil es nicht in die bisherige Denkweise passte); daher werden sich die Verantwortlichen in Deutschland mit dem Artikel 26 schwer tun.

Es gibt viele verschiedene Ausprägungen der gemeinsamen Verantwortlichkeit, wie das Workingpaper „WP 169“ der Artikel-29-Datenschutzgruppe auf Seite 22 beschreibt: *„[Angesichts der Komplexität der heutigen Gegebenheiten der Datenverarbeitung] muss der Begriff ‚gemeinsam‘ im Sinne von ‚zusammen mit‘ oder ‚nicht alleine‘ in **unterschiedlichen Spielarten und Konstellationen** ausgelegt werden“*. [28]

[28] In der deutschen Fachliteratur spielte das Workingpaper „WP 169“ von 2010 lange Zeit eine nur sehr untergeordnete Rolle. Erstmals im „Facebook-Freunde-Finder“-Urteil U 42/12 am 24.01.2014 vom LG Berlin wird das Workingpaper „WP 169“ erwähnt. Dann im Jahr 2016 berichten Fachzeitschriften und Fachbücher erstmals (und zaghaft) über dieses Workingpaper

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

8.1 Benennung eines Datenschutzbeauftragten [GVO_037]

Datenschutzbeauftragten benennen

Gemäß Artikel 37 (1) muss unter bestimmten Umständen ein Datenschutzbeauftragter (DSB) benannt werden. Diese Person wird den Verantwortlichen u.a. über die Pflichten der DS-GVO unterrichten und beraten. Mit Hilfe des Datenschutzbeauftragten wird die Gefahr von Bußgeldern und Schadenersatzforderungen entscheidend minimiert, denn er stellt die notwendige Fachkompetenz zur Verfügung.

Dieser Pflicht wird das Kürzel **[GVO_037]** zugeordnet (siehe Seite 12).

8.1.1 Allgemeine Informationen zur Pflicht [GVO_037]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Bußgeldern** ahnden (siehe Seite 339). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Bußgelder (und ggf. Schadenersatzforderungen) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) bestanden ähnliche Pflichten im Rahmen von § 4f BDSG („Beauftragter für den Datenschutz"). Dort war der Datenschutzbeauftragte bereits seit 1977 verbindlich geregelt. Im Jahr 2006 wurde der Grenzwert von 5 auf 10 Beschäftigte erhöht. In den anderen EU-Staaten war der betriebliche DSB die absolute Ausnahme.

In Deutschland gilt die 10-Mitarbeiter-Grenze gemäß § 38 BDSG-neu auch nach dem 25.05.2018. So gesehen ändert sich nichts. Das Kriterium bezüglich der nicht-automatisierten Verarbeitung durch mindestens 20 Beschäftigte wurde nicht ins BDSG-neu übernommen. Weitere Details werden weiter unten beschrieben.

In Deutschland thematisiert der § 22 Abs. 2 Nr. 4 BDSG-neu die Benennung eines Datenschutzbeauftragten im Gesundheits- und Sozialbereich (siehe Seite 212).

In der **Fachliteratur** (siehe Seite 312) gibt es viele hilfreiche Dokumente: ● Das 2-seitige Kurzpapier-19 der Bayerischen Aufsichtsbehörde. ● Die 12-seitige Praxishilfe „Der Datenschutzbeauftragte nach der DS-GVO" des GDD im November 2016. ● Die 26-seitige Information „Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht" vom Hessischen Datenschutzbeauftragten vom Juni 2017. ● Die 25-seitige Workingpaper „WP 243" der Artikel-29-Datenschutzgruppe. ● GDD-Praxishilfe DS-GVO I.

➔ Ein beispielhaftes Formular findet sich im Kapitel 12.18 auf Seite 292. Dort wird die Benennung ausführlich gestaltet.

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

8.1.2 Was bedeutet diese Pflicht [GVO_037] ?

a) Wann muss/kann ein Datenschutzbeauftragter (DSB) benannt werden?

Die Benennung kann auf verschiedenen Grundlagen beruhen (siehe auch im Formular auf Seite 292):

1.) Gemäß Artikel 37 (1a) müssen **öffentliche Stellen** immer einen DSB benennen.

2.) Gemäß Artikel 37 (1b) müssen jene Unternehmen einen DSB benennen, die im Rahmen ihrer unternehmerischen **Kerntätigkeit** eine umfangreiche, regelmäßige und systematische **Überwachung** von Menschen durchführen.
Der Begriff „Kerntätigkeit" ist zwar im Erwägungsgrund 97 kurz erläutert („Haupttätigkeit"), trotzdem ist dieses wichtige Kriterium äußerst schwammig. Die Artikel-29-Datenschutzgruppe nennt im oben erwähnten Workingpaper zwei Beispiele auf Seite 20: Die Lohn- und Gehaltsabrechnung der Beschäftigten ist KEINE Kerntätigkeit. Die Patientendaten im Krankenhaus sind hingegen eine Kerntätigkeit.
Gemäß Erwägungsgrund 91 im vorletzten Satz gibt es wohl eine (umstrittene) Ausnahme für Gesundheitsberufe und Rechtsanwälte (siehe Seite 143).
Gemäß Erwägungsgrund 24 ist beispielsweise das Nachvollziehen von Internetaktivitäten eine Verhaltensbeobachtung oder nutzungsbezogene Profilbildung.

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

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

9.0 Einleitung

Sonstige Datenschutzvorschriften

Der Artikel 39 (1a) fordert vom Datenschutzbeauftragten, dass er den Verantwortlichen auch in Hinsicht auf „sonstige Datenschutzvorschriften“ unterrichten und beraten soll. Das ist eine weitgehende Forderung, wie die folgenden Kapitel aufzeigen werden.

Aus verschiedenen Gründen kann hier im PrivazyPlan® keine vollständige Liste aller existierenden Datenschutzvorschriften genannt werden. Daher muss jeder Verantwortliche für sich selbst prüfen, ob es zusätzliche Pflichten einzuhalten gilt.

9.1 Europäische Verordnungen

Sonstige Datenschutzvorschriften

Für die nicht-öffentlichen Stellen in Europa sind die folgenden EU-Verordnungen von besonderem Interesse:

9.1.1 EU Datenschutz-Grundverordnung

Die EU Datenschutz-Grundverordnung (DS-GVO) wurde im April 2016 beschlossen und ist am 25.05.2018 in allen Mitgliedsstaaten wirksam. Die resultierenden Pflichten für nicht-öffentliche Stellen in Deutschland werden hier im PrivazyPlan® ausführlich beschrieben. Siehe auch Seite 354.

Bis dahin sollte die EU-Datenschutz-Richtlinie 94/46/EG aus dem Jahr 1995 den Datenschutz in Europa einheitlich regeln. Doch die sehr unterschiedliche Handhabung in den EU-Mitgliedsstaaten sorgte für Probleme, wie der Erwägungsgrund 9 erläutert. Daher wird jene EU-Richtlinie gemäß Artikel 94 **aufgehoben**.

9.1.2 EU ePrivacy-Verordnung… ist in Arbeit

In Brüssel wird derzeit die Privatsphäre in der elektronischen Kommunikation intensiv diskutiert.

Eine ePrivacy-Verordnung („ePrivacyV“) soll noch bis zum 25.05.2018 beschlossen werden. Viele Experten zweifeln an diesem ambitionierten Zeitplan; doch der Beschluss der DS-GVO im April 2016 hat gezeigt, was alles möglich ist, wenn der politische Wille gegeben ist.

Am 10.01.2017 wurde ein EU-Kommission-Vorschlag beschlossen. Am 26.10.2017 wurde ein EU-Parlaments-Vorschlag beschlossen (siehe auch hier und hier). Nun muss sich der EU-Rat dieses Themas annehmen. Anschließend beginnt der Trilog, bei dem sich die drei EU-Gremien einigen müssen. [41]

Neu im Dezember: Die Trilog-Verhandlungen haben wohl Ende November begonnen; es gibt wohl theoretisch die Möglichkeit, dass diese Verordnung am 25.05.2018 wirksam wird. Die Deutsche Bundesregierung ist skeptisch.

In Europa werden dann die DS-GVO und die (zukünftige) ePrivacyV den Datenschutz in Europa einheitlich und verbindlich regeln. Dann ist Europa in jeder Hinsicht ein vereinheitlichter elektronischer Markt.

Bisher gilt noch die Richtlinie 2002/58/EG aus dem Jahr 2002. Wie jede Richtlinie, so ist auch die 2002/58/EG nicht unmittelbar rechtswirksam. Vielmehr müssen die EU-Staaten entsprechende Gesetze erlassen. In Deutschland geschieht dies beispielsweise über das TMG und TKG (siehe weiter unten).

Sobald der Wortlaut der ePrivacyV amtlich feststeht, wird dieser von uns unter www.eprivacy-regulation.eu publiziert.

9.2 Nationale Rechtsvorschriften in den EU-Mitgliedsstaaten

Sonstige Datenschutzvorschriften

Eigentlich soll die DS-GVO den Datenschutz in ganz Europa vereinheitlichen. Die Gesetzesüberschrift erwähnt nicht ohne Grund explizit den „*freien Datenverkehr*“. Doch es gibt viele dutzend Öffnungsklauseln, die den EU-Ländern individuelle Anpassungen erlauben (siehe Seite 354).

... weitere Vorschriften finden Sie in der Vollversion…

[41] Im Januar 2017 wurde ein Entwurf publiziert (mit Übersetzungen in alle EU-Sprachen). Im Oktober 2017 wurde ein neuer Entwurf publiziert.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

10.0 Einleitung

BDSG-neu

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 354).

An diesen Öffnungsklauseln können die nationalen Gesetzgeber die Datenschutzbestimmungen präzisieren und an andere nationale Gesetze anpassen.

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

In der Fachliteratur (siehe Seite 312) gibt es – im August 2018 – noch nicht so viele hilfreiche Dokumente: ● DatenschutzPraxis 07/2017 Seite 17-19.

Die Inhalte dieses Kapitels können sich noch ändern. Im August 2017 ist das BDSG-neu noch zu frisch, als dass abschließende Einschätzungen möglich wären.

10.0.1 Die neue Gesetzgebung („DSAnpUG-EU“)

Der Deutsche Bundestag hat diese gesetzgeberische Möglichkeit im April 2017 intensiv genutzt. Die verschiedenen Entwurfsstadien des DSAnpUG-EU finden sich hier. Das Resultat ist ein in mehrfacher Hinsicht sehr komplexes „Artikelgesetz“, welches auch einem Datenschutz-Profi erstmal vor Rätsel stellt. Der offizielle Text wurde am 05.07.2017 im Bundesgesetzblatt veröffentlicht.

Für die Privatwirtschaft sind die Artikel 1 (teilweise), 7 und 8 relevant. Der Umfang beträgt ca. 13 Seiten, und hat somit ca. 50% des Umfangs vom alten Bundesdatenschutzgesetz (hier).

Im Kapitel 1.4.2 auf Seite 10 finden Sie verschiedene Möglichkeiten, wie Sie auf den Gesetzestext zugreifen können.

Gemäß Artikel 8 des DSAnpUG-EU tritt das BDSG-neu am 25.05.2018 in Kraft. Gleichzeitig tritt das bisherige BDSG explizit außer Kraft.

Falls Ihr Unternehmen gemäß § 4f BDSG-alt bereits einen Datenschutzbeauftragten bestellt hat, so finden Sie auf Seite 180 einige Hinweise, wie damit zukünftig umgegangen werden kann.

➔ Unter www.bdsg2018.de/de stellen wir das BDSG-neu zur Verfügung.

Eine englische Übersetzung findet sich hier.

10.0.2 Wann kommt das BDSG-neu zur Anwendung?

Diese Frage klärt der § 1 Abs. 4 BDSG-neu. Es gilt

1.) generell für alle öffentlichen Stellen in Deutschland,
2.) bei Verarbeitungen in **deutschen Niederlassungen**,
3.) wenn der Verantwortliche dem Anwendungsbereich der DS-GVO unterliegt, wie es der Artikel 3 beschreibt.

⚠ Somit gilt auch für alle **Unternehmen innerhalb der EU/EWR**, sofern die personenbezogenen Daten in einer deutschen Niederlassung verarbeitet werden.

Da der Begriff „**Niederlassung**“ nicht definiert ist, kann hier im Einzelfall eine genaue Prüfung notwendig sein. Die typischen Fragen lauten: Ist es eine selbstständig oder unselbstständige Niederlassung? Hat die Niederlassung etwas mit der eigentlichen Verarbeitung zu tun? Soll der sehr weite Niederlassungs-Begriff des EuGH genutzt werden (wonach – stark vereinfacht gesagt – schon ein Bankkonto in Deutschland ausreichen würde). Siehe Kapitel 3.7.6 im TOM-Guide® (sehr ausführlich auf fünf Seiten).

[Im Rahmen von PrivazyPlan® wird das Dossier „Niederlassung“ angeboten. Dort werden die relevanten Stellen der DS-GVO in konzentrierter Form zusammengestellt. Mit dieser Hilfe ist es leichter möglich, diese weitreichenden Themen besser zu verstehen.]

10.1 Videoüberwachung kenntlich machen [BDSG_004]

BDSG-neu

In Deutschland muss der Verantwortliche gemäß § 4 Abs. 2 BDSG-neu eine Videoüberwachung von öffentlich zugänglichen Räumen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Die betroffenen Personen sollen den Namen und die Kontaktdaten des Verantwortlichen erfahren.

Dieser Pflicht wird das Kürzel **[BDSG_004]** zugeordnet (siehe Seite 12).

10.1.1 Allgemeine Informationen zur Pflicht [BDSG_004]

Die Aufsichtsbehörde kann auf den ersten Blick **kein** Bußgeld verhängen, weil im § 43 BDSG-neu („Bußgeldvorschriften") kein Bezug auf die Videoüberwachung genommen wird. Doch gemäß Artikel 83 (9) kann der gesamte Artikel 83 analog angewendet werden, wenn eine nationale Rechtsordnung keine Geldbußen vorsieht (siehe Seite 339).

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) bestanden ähnliche Pflichten im Rahmen von § 6b Abs. 2 BDSG („Beobachtung öffentlich zugänglicher Räume"), siehe Kapitel 3.2 im TOM-Guide®.

In der **Fachliteratur** (siehe Seite 312) gibt es im August 2017 noch keine Stellungnahmen. Die Gesetzesbegründung bringt keine neuen Erkenntnisse.

10.1.2 Was bedeutet die Pflicht [BDSG_004] ?

Es bleibt also dabei, dass die öffentlichen zugänglichen Bereiche einer Videoüberwachung weiterhin mit Schildern gekennzeichnet werden müssen. Doch ab dem 25.05.2018 muss dies „frühestmöglich" geschehen. Außerdem sind nun auch die Kontaktdaten des Verantwortlichen zu nennen.

10.1.3 Wie erfüllt man die Pflicht [BDSG_004] ?

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: ● Videoüberwachungen im öffentlichen Bereich müssen auch weiterhin kenntlich gemacht werden. ● Nennen Sie auch den Firmennamen und z.B. eine Telefonnummer. ● Spätestens zum 25.05.2018 muss soweit alles geklärt sein.

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 20.

☐ Schulen Sie Ihre Mitarbeiter. Wann immer eine betroffene Person sich vor Ort beschwert, so sollten die Mitarbeiter sachlich und fachlich fundiert antworten können.

☐ Sollten Sie z.B. auf dem Hinweisschild eine Telefonnummer nennen, so stellen Sie sicher, dass die Telefonmitarbeiter geschult sind. Optimalerweise verwenden Sie dafür eine eigene Durchwahl.

b) Durchführung („do")

Wenn die obigen Planungen abgeschlossen sind, so kann diese Pflicht konkret bearbeitet werden.

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 22.

☐ Gibt es die Möglichkeit, dass Sie schon in Broschüren oder Einladungen auf die jeweilige Videoüberwachung hinweisen? Somit wären die betroffenen Personen schon informiert, bevor sie überhaupt nur in die Nähe dieser Bereiche kommen.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

11.0 Einleitung

Pflichten des DSB

Die Voraussetzung ist zunächst, dass das Unternehmen einen Datenschutzbeauftragten benannt hat. Wichtig sind die diesbezüglichen Pflichten des Verantwortlichen.

➔ Siehe [GVO_037] bis [GVO_039b] im Kapitel 8 ab Seite 176.

11.0.1 Was sind KEINE Pflichten des Datenschutzbeauftragten?

⇧ 11 Pflichten des DSB

Insbesondere in Abgrenzung zu den Zeiten des alten Bundesdatenschutzgesetzes fragt sich, ob sich das Tätigkeitsfeld des Datenschutzbeauftragten ändert. Das ist ganz eindeutig zu bejahen.

Der GVO-Kommentar von Gola schreibt in RdNr. 2, 4 zu Artikel 39:

> *„Im Vergleich zu der Aufgabenstellung des Datenschutzbeauftragten nach dem BDSG verzichtet die DS-GVO auf einzelne operative Aufgaben (Mitarbeiterschulung und Vorabkontrolle) und weist dem Datenschutzbeauftragten in erster Linie eine Compliance-Aufgabe zu. […]*
> *Dass eine ausreichende Sensibilisierung und eine nachgewiesene Mitarbeiterschulung stattgefunden haben, ist vom Datenschutzbeauftragten zu kontrollieren.“*

Der GVO-Kommentar von Kühling/Buchner schreibt in RdNr. 22 zu Artikel 39:

> *„Der Datenschutzbeauftragte ist weder für die Schulung der Mitarbeiter, noch für die Ausarbeitung der Datenschutz-Strategien oder die Durchführung der Datenschutz-Folgenabschätzung zuständig. Insgesamt hat er keinerlei Weisungs- oder Entscheidungsbefugnisse gegenüber der ihn benennenden Stelle und damit keine Erfolgsverantwortung, was die Datenverarbeitung angeht. Er muss allerdings den ihm zugewiesenen Aufgaben ordnungsgemäß nachkommen, um sich selbst nicht einem Haftungsrisiko auszusetzen.“*

Der GVO-Kommentar von Paal/Pauly schreibt in RdNr. 6 zu Artikel 39:

> *„Eine mitwirkende Tätigkeit des Datenschutzbeauftragten bei Entwicklung der internen Strategien wird von der DS-GVO hingegen nicht ausdrücklich vorgesehen“*

In diesem Zusammenhang ist auch die Klärung der Verantwortlichkeit von Interesse. Eindeutige Aussagen dazu gibt es nicht (siehe Paal/Pauly in RdNr. 11f zu Artikel 39).

Neu im Dezember: Hat der Datenschutzbeauftragte aufgrund seiner Überwachungs-Funktion einem besonderes Berufsrisiko? Ist er ein „**Überwachungsgarant**“, der für Datenschutzprobleme haftbar gemacht werden kann? Diese Frage wird in der Fachliteratur immer wieder gestellt. Die „Zeitschrift für Datenschutz“ 09/2017 sieht auf Seite 411-414 keine wesentlichen Änderungen im Vergleich zum BDSG. [44] Zurück zum Vorwort

[44] Der Überwachungsgarant wird hier, hier und hier erwähnt und steht in Verbindung zum § 13 StGB und dem Begriff „unechte Unterlassung“. Siehe auch „Zeitschrift für Datenschutz“ 09/2017 auf Seite 411-414, wo keine wesentlichen Änderungen im Vergleich zum BDSG erkannt wird.

11.1 Unterrichtung hinsichtlich der Pflichten [DSB_001]

Pflichten des DSB

Gemäß Artikel 39 (1a) hat der Datenschutzbeauftragte den Verantwortlichen über die Datenschutzvorschriften und dessen konkreten Pflichten zu **unterrichten**. Auch die Mitarbeiter müssen über deren Pflichten in Kenntnis gesetzt werden. Sollte der Verantwortliche auch als Auftragsverarbeiter tätig sein, so muss er über die diesbezüglichen Pflichten unterrichtet werden.

Dieser Pflicht wird das Kürzel **[DSB_001]** zugeordnet (siehe Seite 12).

11.1.1 Allgemeine Informationen zur Pflicht [DSB_001]

Die Aufsichtsbehörde kann wohl eher kein **Bußgeld** gegen den Datenschutzbeauftragten aussprechen, wenn er dieser Pflicht nicht angemessen nachkommen sollte.

Im Bundesdatenschutzgesetz (in der Fassung bis zum 25.05.2018) bestand im weitesten Sinne eine ähnliche Pflicht im Rahmen des § 4g BDSG („Der Datenschutzbeauftragte wirkt auf die Einhaltung des Datenschutzes hin.“).
Darüber hinaus musste er gemäß § 4g Abs. 1 Nr. 1 BDSG die mit der Verarbeitung beschäftigten Personen mit dem Datenschutz vertraut zu machen.

11.1.2 Was bedeutet diese Pflicht [DSB_001] ?

Diese Unterrichtungspflicht des Datenschutzbeauftragten war ein zentraler Auslöser zur Ausarbeitung des PrivazyPlan®. Dementsprechend wurde der PrivazyPlan® von Anfang an auf diese Unterrichtungs-Funktion hin konzipiert.

Die **Ausrichtung nach den ca. 50 konkreten Pflichten** ist ein extrem wichtiger Schritt, um die geforderte Unterrichtung in transparenter Form vornehmen zu können (siehe Seite 11).

Der Verantwortliche muss sich darauf verlassen können, dass der Datenschutzbeauftragte einen vollständigen Überblick über die Pflichten hat, und dass der Datenschutzbeauftragte dies auch in einer gut strukturierten Form kommunizieren kann.

a) Unterrichtung des Verantwortlichen

Der Datenschutzbeauftragte muss den Verantwortlichen über dessen Pflichten zu unterrichten. Das ist sinnvoll, denn nur wenn der Verantwortliche seine Pflichten kennt, dann kann er sie auch einhalten.

Der PrivazyPlan® liefert diesbezüglich eine sehr umfassende Unterrichtung.

Eine monatliche Aktualisierung stellt sicher, dass der Verantwortliche immer auf dem Stand der Dinge ist. Die wichtigsten rechtlichen Neuerungen werden im Kapitel 13.0 auf Seite 299 aufgelistet.

b) Unterrichtung des Auftragsverarbeiters

Das vom Datenschutzbeauftragten betreute Unternehmen kann unter Umständen auch als Auftragsverarbeiter tätig sein (also im Auftrag streng weisungsbezogen die Daten anderer Unternehmen verarbeiten).

In diesem Fall muss das Unternehmen auch über seine diesbezüglichen Auftragsverarbeiter-Pflichten unterrichtet werden. Über die oben genannten Punkte hinaus liefert der PrivazyPlan® hierfür Folgendes:

- Die Pflicht **[GVO_028a]** auf Seite 164 erfüllt dies, denn dort wird beschrieben, dass der Auftragsverarbeiter nur streng nach Weisung tätig werden darf.
- Im Rahmen von PrivazyPlan® wird das Dossier „Auftragsverarbeitung (Auftragnehmer)“ 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.

c) Unterrichtung der Beschäftigten

Der Datenschutzbeauftragte hat auch die Beschäftigten über deren Pflichten zu unterrichten.

Hier gibt es eine gewisse Parallele zur Pflicht **[GVO_032a]**, wonach der Verantwortliche die Beschäftigten „konkret anzuweisen“ hat (siehe Seite 128).

Im Großen und Ganzen gibt der Verantwortliche das firmeninterne Schulungskonzept vor (sprich: **wer** wird **wann** über **welche** Sachverhalte geschult?). Der Datenschutzbeauftragte hat dank des PrivazyPlan® einen guten Überblick über die

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

12.0 Einleitung

Formulare

Die Beschreibung der Pflichten in den Kapiteln 2-10 umfasst immer auch die Frage, wie man die jeweilige Pflicht konkret erfüllen kann.

In vielen Fällen sind ausführliche Checklisten bzw. Statusformulare notwendig. Aus den folgenden Gründen wurden diese Dokumente hier in das Kapitel 12 ausgelagert:

- Die Auslagerung **spart Platz** in den Kapiteln 2-10. Somit bleiben jene Kapitel noch übersichtlich.
- Manche Formulare sind für **verschiedene Pflichten** relevant. Also ist es sinnvoll, solche Formulare auszulagern.
- Die Auslagerung ermöglicht einen **schnellen Überblick** darüber, welche Formulare überhaupt im PrivazyPlan® zur Verfügung stehen.

Die Formulare beginnen jeweils auf einer neuen Seite, damit Sie jedes Formular gezielt ausdrucken können.

Jedes Kapitel beginnt mit einem einleitenden Text. Darunter befindet sich eine schwarz hinterlegte Überschrift; dort beginnt das Formular ganz „offiziell“.

⚠ Bitte passen Sie die Formulare unbedingt Ihren speziellen betrieblichen Belange an. Die von uns gelieferten Beispiele sollen lediglich eine grobe Orientierung geben.

Insofern sind die hier vorgeschlagenen Formulare wirklich nur ein erster Ansatz für Ihre betrieblichen Belange. Es ist ganz explizit gewünscht, dass Sie die Inhalte der Formulare **per Zwischenablage** z.B. in ein MS-Word-Dokument übernehmen. Dort können Sie dann alle Anpassungen an Ihre betrieblichen Anforderungen vornehmen.

Allerdings sollten Sie (wie immer) auf mögliche Updates hier im PrivazyPlan® achten, um sie dann ggf. in Ihr persönliches Formular zu übernehmen.

Hier noch zwei Tipps zu den Dokumenten in MS-Word:

- **Speicher-Datum anzeigen**
  In der Fußzeile der MS-Word-Dokumente sollten Sie unbedingt das Datum der letzten Speicherung einfügen. In MS-Word 2016 funktioniert dies über „Einfügen | Schnellbausteine | Feld… | SaveDate“.
- **Schreibschutz empfehlen**
  Sie können die Formulare vor versehentlichem Überschreiben schützen, indem Sie in MS-Word 2016 im Speichern-Dialog auf den Link „Mehr Optionen…“ klicken und dann auf die Schaltfläche „Tools“ und „Allgemeine Optionen“ anklicken und dann den „Schreibschutz empfehlen“ aktivieren.
  Beim nächsten Öffnen erscheint ein Dialog „Dem Autor wäre es lieber, wenn Sie dieses Dokument mit Schreibschutz öffnen“. Sehr praktisch.

12.1 Basis-Checklisten für den PrivazyPlan®

Formulare

Die folgende Checkliste kann Ihnen helfen sich bestmöglich in die DS-GVO und in den PrivazyPlan® einzuarbeiten.

12.1.1 Grundsätzliches Einlesen in das Sachthema

Wir schlagen vor, Sie beginnen die ersten 2-3 Stunden mit ausführlicher Lektüre:

⚠ Drucken Sie die folgenden Seiten des Anhangs aus:

- die Liste der Verarbeitungsbeispiele ab Seite 266
- die Kurzzusammenfassung aller Pflichten ab Seite 360
- das ausführliche Inhaltsverzeichnis ab Seite 374
- die tabellarische Übersicht aller Pflichten ab Seite 377
- den Index ab Seite 385

… und legen Sie sich diese Ausdrucke griffbereit zur Seite.

☐ Lesen Sie das **Vorwort** ab Seite 4. Dort finden Sie viele wertvolle Hinweise über die DS-GVO und über den PrivazyPlan®.

☐ Setzen Sie sich **Lesezeichen** auf die folgenden beiden Webseiten:
www.privacy-regulation.eu
www.bdsg2018.de
damit Sie jederzeit schnell auf den Originalwortlaut zugreifen können.

☐ Lesen Sie die **allgemeinen Informationen zur DS-GVO** ab Seite 354. Dort finden Sie interessante Details über DS-GVO und über die sprachlichen Schwierigkeiten.

☐ Datenschutz im Rahmen der DS-GVO ist ein **Compliance-Thema**, wie ab Seite 302 ausführlich beschrieben wird.

☐ Lesen Sie die **Kurzzusammenfassung aller Pflichten** ab Seite 360 (bzw. auf dem Papierausdruck, den Sie gemäß der obigen Empfehlung erstellt haben). Wenn Sie dies gelesen haben, dann haben Sie einen guten Eindruck davon bekommen WAS zu tun ist und WIE es zu tun ist.

☐ Einen **Gesamtüberblick über die DS-GVO** erhalten Sie in der gleichnamigen Broschüre hier für 40 €. Die gesamte DS-GVO wird auf 67 Seiten mit 44 Abbildungen erläutert. Kompakter geht es nicht.
Den zusätzlich dort abgedruckten Verordnungstext sollten Sie auf die bekannten Übersetzungsfehler prüfen (siehe Seite 312), oder besser einfach auf www.privacy-regulation.eu zugreifen. Achten Sie darauf, dass Sie die *zweite* Auflage kaufen. Besonders hilfreich ist das dazugehörige **eBook** im PDF-Format auf Deutsch und **Englisch**! Hierfür müssen Sie sich beim Verlag registrieren und dann den „Content-Code“ vom inneren Buchdeckel eingeben.
Weitere Literaturhinweise finden Sie auf Seite 312.

12.1.2 Personelle Entscheidungen treffen und mit den Arbeiten beginnen

Die Realisierung des PrivazyPlan® im betrieblichen Alltag erfordert eine große, unternehmensweite Anstrengung. Zunächst gilt es zu klären, wer an diesen Arbeiten beteiligt wird.

Im Kapitel „Eine grober Plan zur Umsetzung der DS-GVO“ ab Seite 16 werden die Haupt-Akteure konkret genannt:

☐ Geschäftsführer
☐ Datenschutzbeauftragter
☐ Informations-Sicherheits-Beauftragter
☐ Compliance-Beauftragter
☐ Datenschutz-Fachkraft
☐ Datenschutz-„Team“
☐ ggf. Datenschutz-Projektmanager
☐ ggf. EU-Vertreter

Der Verantwortliche ist handlungsfähig, sobald diese „Rollen/Funktionen“ vergeben sind. Die ersten Schritte sind ab Seite 16 ausführlich beschrieben.

Verfügt Ihr Unternehmen über einen Betriebsrat? Dann entschieden Sie, wer dort den Datenschutz gewährleistet.

12.1.3 Grobe Checkliste für die ersten Schritte

Neu im Dezember

a) Erste Schritte der Geschäftsführung

Bevor es an die eigentliche Arbeit geht, so muss die Geschäftsführung zunächst einmal die Weichen stellen:

☐ Die **grundlegenden Fragen** des Kapitels 1.5 auf Seite 14 sollten vorab geklärt werden. Dazu gehört unter anderem die wichtige Frage, ob das hier im PrivazyPlan® vorgeschlagene Mini-Datenschutz-Managementsystem genutzt werden soll (siehe Kapitel 1.10 auf Seite 26)?

☐ Hat die Geschäftsführung die **Kurzzusammenfassung** der ca. 50 Pflichten gelesen, wie sie im Kapitel 14.1 ab Seite 360 beschrieben sind?

☐ Soll der **„grobe Plan“** gemäß Kapitel 1.6.1 auf Seite 16 umgesetzt werden? Dort werden diverse Zuständigkeiten thematisiert (Datenschutzbeauftragter, Compliance-Fachkraft, Informationssicherheits-Fachkraft, …).

☐ Wird die Geschäftsführung eine offizielle **Leitlinie** verabschieden und der Belegschaft bekannt machen? Siehe Kapitel 12.2 auf Seite 235.

☐ Wer soll den PrivazyPlan® **lesen**? Wie wird sichergestellt, dass die relevanten Beschäftigten die monatlichen Änderungen mitbekommen?

☐ Bevor die Pflichten in den Fachabteilungen konkret bearbeitet werden, so sollte die Geschäftsführung vorher die **grobe Planung** durchführen (also das „plan“ im PDCA-Zyklus). Somit wäre sichergestellt, dass die Pflichten im ganzen Unternehmen einheitlich bearbeitet werden. Das spart Zeit und Nerven.
Konkret kann dies bedeuten, dass in dem Mini-Datenschutzmanagementsystem in der PrivazyPlan.xls die „Plan“-Inhalte in allen relevanten Pflichten-Tabellenblättern ausgefüllt werden (siehe Seite 26).

Nachdem die obigen Punkte geklärt sind, können die ca. 50 Pflichten der DS-GVO in Angriff genommen werden.

b) ggf. Datenschutzbeauftragten benennen

Im PrivazyPlan® wurden 10 Pflichten identifiziert, die mit der Benennung und der organisatorischen Einbindung eines Datenschutzbeauftragten zusammenhängen. Im Kapitel 8 ab Seite 176 wird dies alles ausführlich erklärt.

☐ Soll ein Datenschutzbeauftragter aufgrund rechtlicher Pflichten benannt werden (siehe Pflicht **[GVO_037]** auf Seite 177)? Oder soll dies auf freiwilliger Basis geschehen?

c) Verarbeitungen identifizieren / 40 Pflichten bearbeiten

Von den ca. 50 Pflichten der DS-GVO basieren ca. 40 auf der jeweiligen konkreten Verarbeitungen des Verantwortlichen.

Am Beispiel des **Website-Kontaktformulars** wird dies deutlich: (a) Diese Verarbeitung muss im Verarbeitungsverzeichnis dokumentiert werden, (b) verschiedene Informationstexte müssen erstellt werden, (c) die Persönlichkeitsrechte bezüglich Auskunft, Löschung, Korrektur etc. müssen gewährleistet werden… und vieles mehr.

Dementsprechend ist die Identifikation der Verarbeitungen von besonderer Wichtigkeit. Hierdurch wird das „Spielfeld“ des Datenschutzes abgesteckt.

☐ **Identifizieren** Sie die Verarbeitungen. Der PrivazyPlan® liefert hierfür eine recht umfangreiche Liste mit konkreten Beispielen (siehe Seite 266).

☐ Bearbeiten Sie für jede Verarbeitung die ca. 40 Pflichten. Als Arbeitsgrundlage dient sowohl das Verarbeitungs-**Stammblatt** (siehe Seite 270), als auch die MS-Excel-Tabelle **PrivazyPlan.xls** im Rahmen des „Mini-Datenschutz-Managementsystems“ (siehe Seite 26).

d) Informations-Sicherheits-Managementsystem (ISMS)

Der Verantwortliche muss gemäß Artikel 32 die Sicherheit der Verarbeitung risikobasiert planen, dauerhaft sicherstellen und dies regelmäßig überprüfen (siehe die Pflicht **[GVO_032]** auf Seite 124).

Nur mit Hilfe eines ISMS kann dies gelingen. Im Kapitel 13.4 auf Seite 316 ist das Thema „ISMS“ ausführlich dargestellt.

☐ Entscheiden Sie, **welches** ISMS für Sie geeignet ist.

☐ Beginnen Sie zügig damit, dass ISMS **aufzusetzen**. Der Informations-Sicherheits-Beauftragte muss bis zum 25.05.2018 fertig werden.

d) Sonstiges zum Schluss

Ohne einen Anspruch auf Vollständigkeit sollen hier jene Pflichten aufgeführt werden, die irgendwann vor dem 25.05.2017 erledigt werden sollten:

☐ Der „**Nachweis der Einhaltung der** „Grundsätze“ [GVO_005]“ ab Seite 81 muss erbracht werden.

Zurück zum Vorwort

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

13.0 Einleitung

Fachinformationen

Die folgenden Dokumente liefern Fachinformationen zum allgemeinen Verständnis.

Die Reihenfolge der Kapitel folgt keiner besonderen Planung, sondern ergab sich spontan aus dem thematischen Bedarf des PrivazyPlan®.

13.1 Wichtige (rechtliche) Neuerungen

Fachinformationen

Der europäische Datenschutz ist kein „fertiges System“. Es ist ständig mit neuen Rechtsvorschriften und wichtigen gerichtlichen Entscheidungen oder sonstigen Stellungnahmen zu rechnen.

In dem hier vorliegenden Kapitel werden wichtige Neuerungen kontinuierlich dokumentiert.

13.1.1 2017 im dritten Quartal

- 01.11.2017
  Die Artikel-29-Gruppe hat für drei Workingpaper auch deutsche Übersetzungen geliefert (WP 242, WP 243 und WP 244). So langsam fällt es schwer den Überblick über die verschiedenen Workingpaper zu behalten. Daher wurden alle aktuelle Versionen unter http://www.privazyplan.eu/article29/ übersichtlich zusammengefasst. Diese Dokumentsammlung wird zukünftig kontinuierlich gepflegt.

- 03.10.2017
  Die Artikel-29-Gruppe hat am 03.10.2017 einige neue Workingpaper zur Diskussion gestellt (die endgültigen Versionen kommen wohl Ende 2017):
  - „WP 250“ zur Meldung von Datenschutzverletzungen (Artikel 33, Seite 135)
  - „WP 251“ zur automatisierten Entscheidung (Artikel 22, Seite 76)
  - „WP 252“ zu Cooperative Intelligent Transport Systems
  - „WP 253“ zu Bußgeldern und deren Kriterien (Artikel 83, Seite 76)

- 01.09.2017
  Die deutsche Datenschutz-Konferenz (DSK) hat zahlreiche Kurzpapiere veröffentlicht, um die DS-GVO zu kommentieren: Zertifizierungen nach Artikel 42, Informationspflichten gemäß Artikel 13 und Artikel 14 und Recht auf Vergessenwerden gemäß Artikel 17.
  Bei der betrieblichen Umsetzung der DS-GVO sollten diese Kurzpapiere berücksichtigt werden.

- 31.08.2017
  In Österreich wurde das „Datenschutz-Anpassungsgesetz 2018“ verkündet. In 70 Paragraphen auf 31 Seiten werden die Öffnungsklauseln der DS-GVO genutzt. Bezüglich des Datenschutzbeauftragten gibt es keine Spezialregelung. Siehe auch hier.

- 31.07.2017
  Die deutsche Datenschutz-Konferenz (DSK) hat zahlreiche Kurzpapiere veröffentlicht, um die DS-GVO zu kommentieren: Verarbeitungsverzeichnis, Aufsichtsbefugnisse/Sanktionen, Werbung, Drittland-Übermittlung, Datenschutz-Folgenabschätzung, Auskunftsrecht, Marktortprinzip und Maßnahmenplan.
  Bei der betrieblichen Umsetzung der DS-GVO sollten diese Kurzpapiere berücksichtigt werden.

- 17.07.2017
  Im Bundesgesetzblatt 49/2017 vom 24.07.2017 wurden fast 30 Bundesgesetze novelliert. Größtenteils werden bestehende Gesetze auf die DS-GVO angepasst. Besonders umfangreich sind die Änderungen in der Abgabenordnung (9 Seiten) und im SGB X (13 Seiten). Viele Änderungen treten erst am 25.05.2018 in Kraft.

- 11.07.2017
  Der Compliance-Fragebogen der Bayerischen Aufsichtsbehörde steht nun auch in englischer Sprache zur Verfügung (der Deutsche schon ab dem 24.05.2017, siehe unten).

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

13.2 Compliance (regelgetreuer Datenschutz)

Fachinformationen

Den Wert des PrivazyPlan® erkennt man erst dann so richtig, wenn man das rechtliche Umfeld versteht. Das neue europäische Datenschutzrecht stellt sehr hohe Compliance-Anforderungen an die Unternehmen, Behörden und andere Stellen.

13.2.1 Was ist Compliance? Warum ist das Thema wichtig?

Das Thema „Compliance“ ist manchen Lesern möglicherweise bekannt im Zusammenhang mit dem Aktiengesellschafts-Recht, oder in Hinblick auf die Bekämpfung von Insidergeschäften, Kartellverbot, Geldwäsche und Korruption. Doch spätestens durch die EU Datenschutz-Grundverordnung (DS-GVO) wird Compliance für alle Unternehmen relevant.

„Compliance“ ist das Bündel von Maßnahmen, mit denen ein Unternehmen eine rechtskonforme und redliche Führung seiner Geschäfte überwacht und sicherstellt. Das Ziel ist die Vermeidung von Verhaltensweisen, die straf- und bußgeldbewährt sind, bzw. Schadenersatzansprüche auslösen oder schwerwiegende Reputations- oder Vermögensschäden nach sich ziehen.

Vielleicht nicht ganz zufällig fordert der Artikel 5 (1a) genau dies:

> *„Personenbezogene Daten müssen auf **rechtmäßige** Weise und **nach Treu und Glauben** verarbeitet werden“.*

Treffer! Es kann kein Zweifel bestehen: Datenschutz ist ein Compliance-Thema. [54]

Im Rahmen des PrivazyPlan® wird dies in der Pflicht **[GVO_005]** berücksichtigt (siehe Seite 80).

Im englischen Verordnungstext finden sich die Worte „*compliance*“ bzw. „*comply*“ an 79 Stellen.
Die deutsche Übersetzung nutzt die eher unscheinbaren Worte „*einhalten*“, „*erfüllen*“ oder „*im Einklang stehen*“. Es ist schon bezeichnend, dass man in Deutschland kein entsprechendes Wort hat.

In vielerlei Hinsicht lässt die DS-GVO keinen Zweifel darüber, dass Bußgelder und Schadenersatzforderungen drohen (siehe Seite 339).

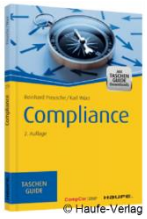
Im Vergleich zu den Zeiten des Bundesdatenschutzgesetzes wird klar: Vorbei sind die Zeiten, wo das Unternehmen aus dem Bauch heraus und auf „gut Glück“ den Datenschutz realisierte; ein Unternehmen kann sich nicht mehr auf deutsche Aufsichtsbehörden verlassen, die nur selten (und sehr moderate) Bußgelder gemäß § 43 BDSG verhängten. Vorbei sind die Zeiten, wo Schadenersatzforderungen gemäß § 7 BDSG nur bei nachweisbaren materiellen Schäden möglich waren.

So gesehen ist Datenschutz-Compliance in Zeiten der DS-GVO kein Luxus, sondern eine wichtige existenzsichernde Maßnahme.

Angesichts der äußerst vielfältigen Transparenzpflichten der DS-GVO sollte ein Verantwortlicher nicht hoffen, dass eventuell rechtswidrige bzw. unredliche Verarbeitungen unentdeckt blieben. Eher das Gegenteil ist zu erwarten. Angesichts

[54] Der Kommentar von Kühling/Buchner geht in RdNr. 15 zu Artikel 5 geht davon aus, dass durch die Formulierung „nach Treu und Glauben“ beispielsweise eine **heimliche** Verarbeitung vermieden werden soll.

der Macht sozialer Netzwerke im Internet (facebook etc.) ist zunehmend zu befürchten, dass negative Erfahrungen der Nutzer bzw. Kunden sich in diesen Foren herumsprechen und zu schwerwiegenden **Reputationsschäden** führen.



© Haufe-Verlag

Sehr empfehlenswert ist das kompakte Büchlein „**Compliance**“ aus dem Haufe-Verlag. Es ist für 7,95 € als Buch oder für 3,99 € als eBook im PDF-Format erhältlich. Dies ist der perfekte Einstieg in das Thema! Auf nur 128 Seiten wird alles erklärt.
Weitere interessante Quellen finden sich hier, hier, hier und hier.

(Im Rahmen von DSB-MIT-SYSTEM® steht ein Newsletter zur Verfügung, um die Mitarbeiter zu sensibilisieren: NEWS_034).

In Deutschland wurden mit dem Wertpapierhandelsgesetz 1994 erstmals Compliance-Anforderungen zur Verhinderung von Insidergeschäften gesetzlich vorgeschrieben. Der Blick ins Ausland zeigt: Die Gesetzgeber anderer Länder sehen die Compliance als unverzichtbar an. In Spanien wurde 2016 ein Unternehmensstrafrecht eingeführt, welches zur Etablierung eines Compliance-Managementsystems verpflichtet. In Italien gibt es sogar ein explizites Compliance-Gesetz.

Mittlerweile interessieren sich auch Kreditinstitute und Versicherungen für das Compliance-Management ihrer Kunden. Beispielsweise für eine Cyber-Versicherung muss ein Informationssicherheits-Managementsystem (ISMS) bestehen (siehe Seite 316).

Weltweit breitet sich der „Compliance-Virus“ immer weiter aus. Durch die DSGVO hat es nun endgültig auch den Datenschutz getroffen.

13.2.2 Wer haftet für Compliance-Verstöße?

Der haftungsrechtliche Ausgangpunkt beginnt wohl beim § 93 AktG bzw. § 43 GmbHG:

> „*Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.*“ [Quelle: § 43 Abs. 1,2 GmbHG]

Konkret haften die Inhaber der Unternehmen (bzw. die führungsverantwortlichen Geschäftsführer) gemäß § 130 OWiG. Sie müssen durch angemessene Aufsichtsmaßnahmen die Verletzung straf- oder bußgeldbewehrter Unternehmenspflichten verhindern.

> *„Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen **Zuwiderhandlungen gegen Pflichten** zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, **die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre**.*
> *Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen. […]*
> *Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. […]“* [Quelle: § 130 Abs. 1 und 3 OWiG]

Durch § 9 OWiG überträgt sich diese Verantwortung (auch) auf die beauftragten Mitarbeiter. Im Rahmen eines BGH-Urteils zu den Berliner Straßenreinigungsbetrieben (5 StR 394/08 vom 17.07.2009) wurde die „Garantenpflicht“ gemäß § 13 Abs. 1 StGB thematisiert (siehe Kapitel 1.5.3 im TOM-Guide®):

> *„Wer es unterlässt, einen Erfolg abzuwenden, der zum Tatbestand eines Strafgesetzes gehört, ist nach diesem Gesetz nur dann strafbar, wenn er rechtlich dafür einzustehen hat, dass der Erfolg nicht eintritt, und wenn das Unterlassen der Verwirklichung des gesetzlichen Tatbestandes durch ein Tun entspricht“*

Gemäß § 30 OWiG können auch Geldbußen bis zu 10 Mio. Euro gegen das Unternehmen als juristische Person verhängt werden.

Manche Unternehmen setzten einen expliziten Compliance-Beauftragten ein (siehe hier), der ggf. teilweise mithaften muss (siehe hier).

In dem obigen Buch „Compliance“ wird auf Seite 25 explizit empfohlen, dass für führende Mitarbeiter eine Vermögensschadenhaftpflichtversicherung (D&O) abgeschlossen werden sollte. Sehr ausführliche Fachartikel erklären die Haftungsrisiken der Unternehmensleitung hier und hier.

Fazit: Die Geschäftsführung hat eine Aufsichtspflicht, um Zuwiderhandlungen gegen bußgeldbewehrte Pflichten zu verhindern oder zumindest wesentlich zu erschweren. Dies lässt sich (zumindest teilweise) auf sorgsam ausgewählte Aufsichtspersonen delegieren (sofern diese überwacht werden).

13.2.3 Wie stellt man Compliance sicher?

Die dauerhafte Sicherstellung von Compliance ist ein aufwändiges Unterfangen. Insbesondere in Hinblick auf die Bekämpfung von Korruption und Geldwäsche existiert ein umfangreicher Markt an Literatur und Software. Es stellt sich hier generell die Frage nach einem Compliance-Managementsystem (CMS).

© Beck-Verlag

Erfreulicherweise steht seit März 2017 ein Fachbuch speziell für den Datenschutz zur Verfügung. Das Buch „Datenschutz-Compliance nach der DS-GVO“ der Autoren Sachs / Kranig / Gierschmann gibt auf 226 Seiten einen sehr guten Einblick für günstige 44 € (auf Papier oder als PDF-eBook).

Bemerkenswert konkret wird auf alle wichtigen Bestandteile eingegangen. Das Buch ist 100%-ig empfehlenswert für alle Unternehmen, die ernsthaft ein Compliance-Managementsystem einführen wollen.

Auf 226 Seiten kann man natürlich keine Vollständigkeit erwarten. Beispielsweise vermisst man die Pflichten des Datenschutzbeauftragten, die natürlich ebenfalls von einem CMS abgebildet werden müssen.

Weiterführende Literatur findet sich beispielsweise im Fachbuch „Das wirksame Compliance-Management-System“ für 52 € als eBook oder auf Papier. Interessant könnte auch das Fachbuch „Praxiswissen Compliance“ aus dem Haufe-Verlag sein für 49,95 auf Papier oder 44,99 als eBook (PDF oder EPUB).

Mit der **DIN ISO 19600** steht ab Mitte 2016 ein internationaler CMS-Standard zur Verfügung; inhaltlich stimmt dieser Ansatz weitgehend mit dem Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer (IDW) überein. Eine 52-seitige Broschüre der DIN erklärt die Hintergründe anhand von 21 Fragestellungen (20 € für Buch & PDF-eBook). [55]

Fazit: Zum Thema „Compliance“ gibt es reichlich Literatur und Knowhow. Leider erfordert der Aufbau eines echten Compliance-Managementsystems (CMS) recht viel Zeit, Geld und Beharrlichkeit.

13.2.4 Compliance durch PrivazyPlan®?

Ab August 2017 wird zur Realisierung der DS-GVO der PrivazyPlan® angeboten. Inwieweit führt er zu Datenschutz-Compliance?

Die zugrundeliegende Idee ist Folgende: Wenn der Verantwortliche alle Pflichten der DS-GVO identifiziert, und diese dann auch einhält, dann sind alle Gefahren von Bußgeldern und Schadenersatzforderungen im Prinzip unter Kontrolle. Das Unternehmen ist Datenschutz-Compliant (insbesondere wenn durch einen PDCA-Zyklus dies dauerhaft kontrolliert und optimiert wird).

Insofern kann der PrivazyPlan® tatsächlich Compliance-Verstöße prinzipiell verhindern helfen.

Durch die sehr weitgehende Rechenschaftspflicht gemäß Artikel 5 (2) muss der Verantwortliche seine Strategien und Maßnahmen dokumentieren. Nur dann kann eine Aufsichtsbehörde gemäß Artikel 83 (2) das Bußgeld entsprechend reduzieren (siehe Seite 339). Auch hier gilt nun also der altbekannte Grundsatz „*Wer schreibt, der bleibt*“. Auch dies leistet der PrivazyPlan®.

Doch damit allein ist noch kein Compliance-Management-System eingerichtet. Der PrivazyPlan® gibt keine Antwort auf die Frage, wie der Verantwortliche sein Unternehmen als Ganzes ausrichten muss, damit das Compliance-„Umfeld“ gegeben ist. Diesen Aspekt findet man eher im obigen Kapitel.

13.2.5 Was ist zu tun?

Die Wichtigkeit von Datenschutz-Compliance ist wohl unumstritten. Doch wie soll man vorgehen?

[55] Auf Seite 36 der Broschüre werden die Grundprinzipien übersichtlich grafisch dargestellt.

1. In welchen Bereichen will das Unternehmen seine Compliance verbessern?

   Zunächst gilt es zu klären, welche Themengebiete in Zukunft in Angriff genommen werden sollen. Beispielsweise die folgenden Sachgebiete kämen dafür in Frage:
   Arbeitssicherheit, Brandschutz, Datenschutz, Export- und Importkontrolle, Geldwäscheprävention, Korruptionsprävention, Produktsicherheit, Qualitätsmanagement, Vertragsmanagement, unlauterer Wettbewerb, Umweltschutz, Wirtschaftskriminalität und Zoll.

2. Wie umfangreich soll das Compliance-Management ausfallen?
   Die Menge der zu kontrollierenden Bereiche (siehe oben) hilft bei der Entscheidung, wie komplex das Compliance-Management sein darf. Je mehr Bereiche abgedeckt werden sollen, desto systematischer muss der Verantwortliche dem Thema begegnen. Jetzt wäre es Zeit sich fachkundig zu machen und externe Expertise einzuholen.
   In Bezug auf den Datenschutz wird das oben erwähnte Fachbuch „Datenschutz-Compliance nach der DS-GVO“ ausdrücklich empfohlen.

3. Konzentration auf das Wesentliche? Der PrivazyPlan®.
   Das Unternehmen hat keine Ressourcen für ein „echtes“ Compliance-Managementsystem mit allem Drum und Dran? Dann sollte der Verantwortliche mindestens die Kern-Pflichten der DS-GVO in Angriff nehmen. Somit lassen sich die unmittelbaren Bußgeld- und Schadenersatz-Gefahren kontrollieren. Genau hierfür ist der PrivazyPlan® konzipiert.

4. Beginn der Arbeiten
   Es gilt zügig zu handeln. Bis zum 25.05.2018 hat der Verantwortliche Zeit, um die Datenschutz-Compliance herzustellen (und nachweisbar zu machen). Aus Sicht von PrivazyPlan® sieht die Vorgehensweise folgendermaßen aus:

   (a) Konkrete Pflichten aus der DS-GVO extrahieren. Diesen Schritt hat PrivazyPlan® bereits erfüllt.

   (b) Pflichten mit Prioritäten versehen (Mut zur Lücke?). Hierfür hat PrivazyPlan® bereits ein Priorisierungs-Konzept vorgesehen. Siehe Seite 16.

   (c) Beginn mit den zeitaufwändigen Pflichten. Im Rahmen von PrivazyPlan® sind die zeitaufwändigen Pflichten benannt.

   (d) Für jede einzelne Pflicht der DS-GVO gilt: Erst planen, dann vorbereiten und dann durchführen.. Hierfür bietet PrivazyPlan® konkrete PDCA-Checklisten. Siehe Kapitel 12 ab Seite 230.

   (e) Vorbereiten und anwenden von Checklisten und Statusblättern. Hierfür bietet *PrivazyPlan®* konkrete PDCA-Checklisten. Siehe Kapitel 12.

   (f) Einsetzen eines Datenschutzbeauftragten, der die Compliance überwacht. Die konkreten DS-GVO-Aufgaben des Datenschutzbeauftragten sind im Kapitel 11 des PrivazyPlan® beschrieben. Mit Hilfe der Software DSB-Reporter® kann die Pflichterfüllung (risikoorientiert) überwacht werden.

   Parallel zu diesen Arbeiten sollte der Verantwortliche überlegen, ob er ein Datenschutz-Ticket-System einführen will (siehe Seite 343). Das gleiche gilt für ein zentrales Dokumenten-Managementsystem (siehe Seite 344).

Es gibt viel zu tun. Packen wir's an!

13.2.6 Ultrakurz-Checkliste zur Datenschutz-Compliance

Wie kann man (zumindest ganz grob) abschätzen, ob ein Unternehmen datenschutzkonform arbeitet? Angesichts der enormen Komplexität des Themas kann eine Checkliste wirklich nur die ganz elementaren Fragen anreißen. Da die Datenschutz-Compliance eine beständige Arbeit im Sinne des PDCA-Zyklus erfordert, wird die folgende Checkliste nach diesem Muster gegliedert:

a) Planung einer Strategie („plan“)

Die folgenden Fragestellungen haben einen Planungs-Charakter. Hier werden die grundsätzlichen Entscheidungen getroffen und Weichen gestellt:

1.) Hat sich die Geschäftsführung ganz klar und „offiziell“ dem Ziel der Datenschutz-Compliance verschrieben? Ist ein „echtes Datenschutz-Compliance-

Management“ geplant, oder lediglich eine Erfüllung der wichtigsten konkreten Pflichten? Gibt es eine entsprechende Leitlinie?

2.) Gibt es klar erkennbare personelle Strukturen, die erkennen lassen, dass das Unternehmen die verantwortlichen und zuständigen Beschäftigten benannt hat? Gibt es einen Compliance-Officer? Gibt es ein Team mit Experten aus allen Fachabteilungen? Sind die Rechte und Pflichten dieser Beschäftigten schriftlich geregelt und mit Unterschriften versehen?

3.) Wie gelangen die Beschäftigten an die notwendige Fachkunde? Wird ausreichend Fachliteratur beschafft, oder Fortbildungsveranstaltungen genutzt? Stellt der Datenschutzbeauftragte notwendiges Knowhow zur Verfügung (z.B. in Form des TOM-Guide®)?

4.) Besteht ein Datenschutz-Ticketsystem, um Anliegen der betroffenen Personen zeitnah, zuverlässig und nachvollziehbar zu bearbeiten?

5.) Existiert ein Dokumenten-Managementsystem, um alle notwendigen Texte, wie Gesetzestexte, Vereinbarungen, Einwilligungstexte, Checklisten (blanko und ausgefüllt) zentral abzulegen?

6.) Der EU-Datenschutz ist kein „fertiges System“. Wie wird auf rechtliche Änderungen reagiert? Wer ist zuständig alle relevanten Neuerungen zu suchen und dem Unternehmen zur Verfügung zu stellen?
Betroffen sind Änderungen an (a) der DS-GVO und (b) an nationalen Gesetzen aller EU-Länder, die das Unternehmen mit Waren oder Dienstleistungen beliefert und (c) Stellungnahmen der Artikel-29-Datenschutzgruppe und (d) Stellungnahmen der deutschen Aufsichtsbehörden und (2) gerichtliche Entscheidungen… und vieles mehr.

7.) Wurde ein Datenschutzbeauftragter (mit der notwendigen Fachkunde und Zuverlässigkeit) benannt? Falls dies nicht notwendig ist (und auch nicht freiwillig geschehen soll): Wer ist im Unternehmen der Datenschutzexperte?

8.) Welche Aufgaben übernimmt der Datenschutzbeauftragte? Hat der Verantwortliche ein genaues Bild davon, was der Datenschutzbeauftragte liefert? Wie nimmt er seine Pflicht zur Unterrichtung, Beratung und Überwachung wahr? Was liefert der Datenschutzbeauftragte nicht?

b) Durchführung („do“)

Im Folgenden geht es um die konkrete Durchführung. Jetzt wird der Datenschutz im Arbeitsalltag der Beschäftigten spürbar:

1.) Sind die Beschäftigten über die DS-GVO und andere Rechtsvorschriften informiert? Gab es Schulungen? Sind Newsletter geplant?

2.) Hat der Verantwortliche einen präzisen Überblick über alle (mindestens 50) konkreten rechtlichen Pflichten der DS-GVO und anderer Rechtsvorschriften? Wie wird den Beschäftigten das notwendige Datenschutz-Knowhow vermittelt, damit diese die jeweilige Pflicht verstehen? Ohne diese Detailkenntnisse ist Compliance unmöglich. Beispielhaft seien einige ganz besonders „kritische“ Pflichten genannt:
- Informations-Sicherheits-Managementsystem (ISMS),
- Verarbeitungsverzeichnis,
- Ermöglichen von Daten-Kopien und Daten-Export

3.) Werden die Pflichten priorisiert? Werden die zeitlich aufwändigen Pflichten zuerst begonnen? Gibt es für die Erfüllung der Pflichten konkrete zeitliche Ziele? Gibt es eine Form von Projektmanagement, um die zeitliche Einhaltung der Pflichterfüllung zu kontrollieren. Stichtag ist der 25.05.2018.

4.) Wie werden die als relevant erkannten Pflichten bearbeitet? Gibt es eine systematische Vorgehensweise? Wer bestimmt darüber, wie die jeweilige Pflicht erfüllt werden kann. Gibt es Checklisten und eine Gliederung im Sinne des PDCA-Zyklus?

5.) Wird das Verarbeitungsverzeichnis gemäß Artikel 30 ordnungsgemäß geführt? Hat die zuständige Person die notwendige Fachkunde und den notwendigen Überblick, um alles korrekt zu dokumentieren? Wird das Ergebnis den Fachabteilungen in angemessener Form zugeleitet, damit diese korrekt arbeiten können?

Der PrivazyPlan® liefert ca. 50 konkrete Pflichten, die der DS-GVO und anderen Rechtsvorschriften (StGB, TMG, TKG, UWG, …) entnommen sind. Jede Pflicht hat ein eigenes Kürzel (z.B. „GVO_015“); somit ist eine systematische Bearbeitung sehr einfach möglich. Jede einzelne Pflicht wird im Kapitel 2-10 erklärt und die Bearbeitung angeleitet. Das Kapitel 12 liefert Checklisten und Statusblätter.

c) Kontrolle („check“)

Im Sinne des PDCA-Zyklus erfordert die dauerhafte Datenschutz-Compliance eine ständige Kontrolle. Dies ist auf verschiedene Weisen möglich:

1.) Wie nimmt die Geschäftsführung ihre Überwachungspflicht gemäß beim § 93 AktG bzw. § 43 GmbHG und § 130 OWiG wahr? Geschieht dies „passiv“ über ein quartalsmäßiges Berichtswesen, und auch „aktiv“ über halbjährliche Meetings?

2.) Gibt es ein internes Kontrollsystem, wo der Compliance-Manager (oder andere Beschäftigte des Unternehmens) kontrollieren, ob die jeweils zuständigen Kollegen die ihnen zugeordneten Pflichten erfüllen? Auf diese Weise wird recht engmaschig kontrolliert, ob z.B. der „Daten-Export-Manager“ wirklich sicherstellt, dass die Daten einer betroffenen Person wirklich auf Anforderung geliefert werden können. Gibt es ein regelmäßiges Berichtswesen?

3.) Wie nimmt der Datenschutzbeauftragte seine Überwachungspflicht gemäß Artikel 39 (1b) wahr? Kontrolliert er den Verantwortlichen systematisch auf die Einhaltung dessen (ca. 50) Pflichten? Prüft er auch systematisch die übergeordneten Strategien des Verantwortlichen? Gibt es ein regelmäßiges Berichtswesen?
(Siehe Pflicht [DSB_003] auf Seite 225.)

4.) Werden Zertifizierungen im Sinne des Artikels 42 angestrebt?

d) Verbesserung („act“)

Wie wird auf Compliance-Optimierungsbedarf reagiert?

1.) Wenn der Geschäftsführer Optimierungsbedarf sieht: Informiert er ggf. die anderen Geschäftsführer? Hat er ein Budget, um Software oder Know-how zu beschaffen oder neue Personen zu beschäftigen? Falls er die betriebliche Organisation ändert: Wird dies dokumentiert, um einer Aufsichtsbehörde beweisen zu können, dass der Datenschutz wirklich „lebt“?

2.) Wie melden die eigenen Beschäftigten im Rahmen des internen Kontrollsystems Ihre Optimierungsvorschläge? Wird dies zunächst mit dem Datenschutzbeauftragten besprochen? Wird anschließend die Leitung der Fachabteilung (und ggf. auch die Geschäftsführung) informiert?

3.) Wie meldet der Datenschutzbeauftragte seine Optimierungsvorschläge? Die Geschäftsführer formulieren diesbezüglich zunächst Vorgaben bezüglich des Schweregrades, der Dringlichkeit, und der zu informierenden Personen oder Abteilungen. Somit kann der Datenschutzbeauftragte nach objektiven Kriterien die gewünschten Rückmeldungen geben.

Im Mai 2017 hat die Bayerische Datenschutz-Aufsichtsbehörde einen Fragebogen entworfen, der die Compliance mit der DS-GVO abfragt; somit wissen die Unternehmen nun, welche Art von Fragen auf sie zukommen werden.

13.2.7 Software für Compliance

Am Software-Markt gibt es so verschiedene Software-Programme, um Compliance zu gestalten und zu leben. Im Folgenden sollen zwei beispielhafte Produkte erwähnt werden:

a) viflow

Die ViCon GmbH aus Hannover stellt eine ganze Produktreihe zur Verfügung, um Compliance-Angelegenheiten zu bearbeiten.

- Das Produkt „viflow“ basiert auf MS-Visio und kann den compliance-konformen Umgang mit Personenbezogenen Daten grafisch visualisieren. Die Grafiken werden auf einem MS-Windows-PC erzeugt und können dann als HTML-Dateien allgemein genutzt werden. Die Lizenz für 5 User beginnt bei 690 € (einmaliger Kaufpreis).
- Ergänzt wird dies durch „viflow easy plan“, in welchem die Pflichten in Form von Aufgaben formuliert werden. Die Lizenz für 3 User beginnt bei 990 € (einmaliger Kaufpreis).
- Die anfallenden Text-Dokumente können mit „viflow DMS“ in einem Dokumenten-Managementsystem übersichtlich abgelegt werden. Die Lizenz für 5 User beginnt bei 1.290 € (einmaliger Kaufpreis).

b) Das GEORG Compliance Management System

Die Martin Manz GmbH aus Großwallstadt bietet den „GEORG Compliance Manager“. Mit dieser Software lassen sich umfangreiche Compliance-Managementsysteme einrichten. Es ist konzipiert z.B. für den Bereich „Arbeitssicherheit“ und

bietet dort viele hundert Pflichten, die das Unternehmen erfüllen und dokumentieren kann. [Leider konnten bisher noch keine konkreten Preise in Erfahrung gebracht werden…]

c) DocSetMinder®

Die GRC Partner GmbH aus Kiel bietet das Produkt DocSetMinder® an. Es basiert auf einer relationalen Datenbank (MS SqlServer) und ist mit MS-Windows-Clients bedienbar. Auf der Basis von frei gestaltbaren Vorlagen lässt sich das Unternehmen (mit Standorten, Mitarbeitern etc.) dokumentieren und dann basierend darauf durch verschiedene Compliance-Module ergänzen. Der Aufbau ist sehr übersichtlich uns intuitiv bedienbar. Der Umsetzungsstatus im Rahmen von PDCA-Zyklen ist darstellbar. Die systematische Dokumentation z.B. von Datenschutzverletzungen ist möglich. Die ca. 50 Pflichten des PrivazyPlan® ließen sich vermutlich leicht implementieren und konkret bearbeiten.

Das Grundmodul kostet (für 5 User) einmalig 6.500 € und jährlich ca. 1.200 € für Wartung und Updates. Die Zusatzmodule (Reporting, Termine/Aufgaben, Im-/Export, IT-Landschaft, BSI-Grundschutz, ISO-27001, ISIS-12, Arbeitsschutz, …) kosten jeweils ca. 2.000 bis 4.000 €. Es gibt auch ein Datenschutz-Modul, welches gemeinsam mit dem ULG entwickelt wurde.

d) Customer-Relation-Management-Software (CRM) zweckfremd nutzen

Vermutlich verfügt jedes CRM über alle Features, die man auch für ein Compliance-Managementsystem benötigt. Es gibt Opensource-Systeme wie beispielsweise 1CRM, die kostenlos zur Verfügung stehen. Die Installation auf einem Server mit PHP und mySQL geht leicht von der Hand.
Wie kann man nun die Leistungsmerkmale eines CRM für die Datenschutz-Compliance zweckentfremden?

- In den „Kunden“-Formularen wird das eigene Unternehmen gespeichert (und ggf. auch die anderen Unternehmen der Unternehmensgruppe).
- Die „Kontakte“ sind nicht (potentielle) Kundenkontakte, sondern die eigenen Mitarbeiter. Hier können die wichtigsten Führungspersonen und sonstige zuständige Personen hinterlegt werden. Somit stünden sie für verschiedenste Zwecke zur Verfügung (z.B. für die Vergabe von Zuständigkeiten, aber auch als Adressaten von E-Mail-Rundschreiben).
- Die E-Mail-Kampagnen würde man nicht nutzen, um Kunden zu gewinnen, sondern um die eigenen Beschäftigten zu sensibilisieren.
- Der E-Mail-Client kann genutzt werden, um datenschutzrelevante E-Mails (z.B. für datenschutzverletzung@unternehmen.de) gemeinsam zu bearbeiten.
- Die „Servicefälle“ werden genutzt, um Anliegen der betroffenen Personen (auf Auskunft, Widerruf etc.) zu dokumentieren und zu bearbeiten.
- Die Datei-Versionierung kann genutzt werden, um Einwilligungserklärungen und Informationstexte zu speichern und deren Verlauf dauerhaft nachweisen zu können.
- Die Aufgabenverwaltung würde das Datenschutz-Team nutzen, um gemeinsam die Aufgaben zu erledigen.
- Der Team-Kalender kann genutzt werden, um das Datenschutz-Team zu koordinieren. Es lassen sich auf ganze Fortbildungs-Veranstaltungen planen und durchführen.
- Die Projektplanungs-Features können vom Datenschutz-Projektmanager genutzt werden, um die Umstellung auf die DS-GVO zu planen und die terminlichen Ziele zu realisieren.
- Das Ticket-System wird genutzt, wenn die Überwachung der Pflichten einen Verbesserungsbedarf erkennen lässt.
- Könnte man sogar das Verarbeitungsverzeichnis in einem CRM ablegen? Nun, dafür müsste man die bestehenden Daten-Strukturen schon arg strapazieren. Mittels der benutzerdefinierten Datenfelder könnte man z.B. im Diskussion-Thread entsprechende Strukturen schaffen, um z.B. den Zweck und die Löschfristen einer Verarbeitung zu dokumentieren. [Vielleicht findet sich aber auch ein Programmierer, der ein entsprechendes Add-On programmiert…]

Schon diese kurze Liste der Anwendungsmöglichkeiten zeigt: Ein CRM kann auch gut zum Compliance-Management genutzt werden. Es bedarf lediglich etwas Fantasie.

13.2.8 Fazit zum Thema „Compliance“

Fassen wir das Thema „Compliance“ zusammen:

❶ Was ändert sich zum 25.05.2018 hinsichtlich Compliance?

- **Nachweispflicht** (Es reicht nicht mehr aus, dass man den Datenschutz einfach nur einhält. Vielmehr muss man dies gemäß Artikel 5 (2) jederzeit nachweisen können. Diese „Nachweispflicht“ wird von der Fachliteratur gemeinhin mit „Compliance“ gleichgesetzt.)
- **Systematische Sicherheit** (Die technisch-organisatorischen Maßnahmen bedürfen gemäß Artikel 32 (1d) einer „regelmäßigen Überprüfung, Bewertung und Evaluierung“. Dies erfordert einen PDCA-Zyklus. Das ist Compliance pur.)
- **Strategien entwickeln** (Sie müssen gemäß Erwägungsgrund 78 „interne Strategien festlegen“, um die Einhaltung der Verordnung nachweisen zu können. Das läuft auf den PDCA-Zyklus hinaus.)
- **Risiken beherrschen** (Nicht zuletzt die Datenschutz-Folgenabschätzung des Artikel 35 setzt einen bewussten Umgang mit Risiken voraus. Unter Umständen sind sehr detaillierte Abwägungen durchzuführen.)
- **Datenschutzbeauftragter überwacht Strategien** (Der Datenschutzbeauftragte hat gemäß Artikel 39 (1b) u.a. auch die Strategien des Verantwortlichen zu überwachen. Alle Pflichten des Datenschutzbeauftragten finden sich ab Seite 221.)
- **Pflichten erfüllen** (Bedingt durch die obigen Belange muss die DS-GVO in ihre einzelnen Pflichten zerlegt werden. Genau dies liefert der PrivazyPlan®. Ab Seite 360 finden Sie eine kurze Charakterisierung aller ca. 50 Pflichten.)

  Fazit: Bis zum 25.05.2018 zielte das Bundesdatenschutzgesetz allein auf das Ergebnis ab („Das BDSG muss eingehalten werden“).

  Die DS-GVO reglementiert nun auch den Weg dorthin (Dokumentation, Risikoabschätzung, Strategien, regelmäßige Überprüfung mittels PDCA, Nachweispflicht).

❷ Warum lohnt sich Compliance?

- **Vermeidung von Bußgeldern** (immerhin bis zu 4% vom konzernweiten Jahresumsatz)
- **Vermeidung von Schadenersatzforderungen** (neuerdings auch für immaterielle Schäden)
- **Vermeidung von Prüfungen durch die Aufsichtsbehörden** (weil dies mehrere Manntage an Arbeitszeit verschlingt, und weil externe Ressourcen wie z.B. ein Datenschutzbeauftragter ebenfalls den Arbeitsaufwand entlohnt bekommen).
- **Vermeidung von negativer Berichterstattung** (in Zeiten von facebook und Co. ist dies ein wichtiges Argument, weil in kürzester Zeit ein mühevoll aufgebautes Image zerstört werden kann)
- **Unverzichtbarer Aspekt Ihrer Dienstleistung?** (Wenn Ihr Unternehmen auch Umsatz damit macht, dass Sie personenbezogene Daten für andere Unternehmen verarbeiten, dann müssen Sie auch Datenschutz liefern. Ohne einen nachweisbaren Datenschutz haben Sie am Markt vielleicht bald keine Chancen mehr. Wundern Sie sich nicht, wenn Sie keine neue Aufträge erhalten und bestehende Verträge gekündigt werden bzw. auslaufen.)
- **Abwenden von Geschäftsrisiken** (Es wird nicht lange dauern, da wird Ihr Wirtschaftsprüfer auch den Datenschutz mit seinen hohen Bußgeld- und Schadenersatzforderungen entdecken. Sie werden ihm nachweisen müssen, dass diese Risiken unter Kontrolle sind.
  Ähnliches blüht Ihnen auch, wenn Sie Ihr Unternehmen veräußern möchten: Ein mangelnder Datenschutz wird garantiert zu (unverhältnismäßig) hohen Abschlägen der Kaufsumme führen.)

- **Aus Überzeugung** (Ja, auch das gibt es. Manche Inhaber von Unternehmen stehen auf dem Standpunkt: „Ich selbst verlange für mich einen wirksamen Datenschutz. Wie könnte ich dies meinen eigenen Beschäftigten und Kunden verweigern?“ Respekt.)

❸ Wann legen Sie los?

- **Warten auf die Krise** (Sie hoffen „Nichts wird so heiß gegessen, wie es gekocht wird“. Sie hoffen, dass schon niemand merken wird, dass Sie nicht DSGVO-compliant sind. Sie glauben, dass man die ca. 50 Pflichten auch dann noch erfüllen kann, wenn man erwischt wurde. Das ist riskant. Und teuer.)

- **Warten auf „*die* Lösung“** (Sie sehen die Relevanz durchaus ein, aber Sie warten erstmal, ob es nicht einen Dienstleister gibt, der Ihnen alles „fressfertig“ liefert. Sie brauchen nicht mehr länger warten, denn einen konkreteren Plan als den PrivazyPlan® werden Sie so schnell nicht finden. Also legen Sie los!)

- **Hier und jetzt !** (Sie gehen in die Offensive. Nutzen Sie den PrivazyPlan® und starten Sie einfach durch. Je früher Sie anfangen, desto weniger Druck haben Sie. Somit haben Ihre Beschäftigten mehr Zeit und haben weniger Druck… so vermeiden Sie Burnout und „innere Kündigungen“.)

❹ Was ist konkret zu tun?

- **Bekenntnis geben** (Die Geschäftsführung erklärt schriftlich, dass der Datenschutz ein wichtiges Unternehmensziel ist. Nur so wird das Unternehmen auf Compliance-Kurs gebracht.)

- **Organisation aufbauen** (Welcher Mitarbeiter wird Ihr „Compliance“-Officer? Er wird die Zügel in die Hand nehmen und auf die Einhaltung der Datenschutz-Compliance hinwirken. Ernennen Sie eine Kontaktperson in jeder Fachabteilung. Bilden Sie ein Team!)

- **Datenschutzbeauftragten benennen** (Benennen Sie einen Datenschutzbeauftragten, der Sie gemäß Artikel 39 bezüglich Ihrer Pflichten unterrichtet, berät und überwacht. Wenn er nicht selbst über ein fertiges Konzept verfügt, so schauen Sie sich gemeinsam den PrivazyPlan® an.)

- **Fachkunde erlangen** (Nutzen Sie den PrivazyPlan®, um sich fachlich fit zu machen. Starten Sie im Kapitel 14.1 ab Seite 360, denn dort finden Sie die kürzest mögliche Darstellung der ca. 50 Pflichten. Nutzen Sie die Liste der Fachliteratur und Informationsquellen auf Seite 312.)

- **Pflichten identifizieren und priorisieren** (Ab Seite 360 finden Sie eine kurze Charakterisierung aller ca. 50 Pflichten. Welche Pflichten sind langwierig? Welche müssen bis zum 25.05.2018 erledigt sein? Wo drohen besonders hohe Bußgelder? Welche Fehlverhalten bleiben garantiert nicht unentdeckt? Das Datenschutz-Team setzt die Prioritäten und gibt diese in die Fachabteilungen.)

- **Pflichten abarbeiten** (Vergeben Sie die Zuständigkeiten in den Fachabteilungen: Welche Mitarbeiter sollen welche Pflichten konkret bearbeiten? Die jeweiligen Pflichten sind im PrivazyPlan® ganz sauber getrennt behandelt; eine Verteilung auf mehrere Mitarbeiter ist kein Problem. Setzen Sie zeitliche Ziele und überwachen Sie diese.)

❺ Könnte das alles nicht der Datenschutzbeauftragte erledigen?

Nein, aus den folgenden Gründen wäre das **nicht zulässig**:

- **Interessenkonflikt** (Die Aufgaben des Datenschutzbeauftragten sind im Artikel 39 genau aufgelistet. Der Aufbau eines Datenschutz-Compliancesystems gehört nicht dazu. Im Gegenteil: Die „Überwachungs“-Funktion verbietet es geradezu, dass der Datenschutzbeauftragte jene Inhalte erstellt, die er dann später überwachen soll.
Im Krisenfall würde die Aufsichtsbehörde die Wirksamkeit seiner Überwachungsfunktion in Zweifel stellen. Eine wichtige Säule des Datenschutzes wäre in Gefahr.)

- **Unabhängigkeit und Weisungsfreiheit** (Gemäß Erwägungsgrund 97 soll der Datenschutzbeauftragte seine Pflichten und Aufgaben in „vollständiger Un-

abhängigkeit“ ausüben können. Gemäß Artikel 38 (3) dürfen dem Datenschutzbeauftragten „keine Anweisungen“ erteilt werden.
Was würde passieren, wenn der Datenschutzbeauftragte weisungsfrei und in völliger Unabhängigkeit die Compliancemaßnahmen für das Unternehmen gestalten würde? Er würde dem Unternehmen ein Compliance-Managementsystem nach freiem Ermessen diktieren; jede fachliche Einflussnahme des Unternehmens wäre unmöglich. Ist das gewollt?

Und darüber hinaus wäre es auch nicht praktikabel:

- Keine **detaillierten Prozesskenntnisse** (Die Datenschutzmaßnahmen müssen in die bestehenden Prozesse eingeflochten werden (z.B. Mitarbeiter-Einstellung, Kundenbetreuung, Kaltakquise). Doch nur Sie selbst wissen, wie Sie hier genau vorgehen und worauf es ankommt. Wollen Sie von Ihrem Datenschutzbeauftragten verlangen, dass er sich im Detail in alle Ihre Geschäftsprozesse einarbeitet, damit er die passenden Datenschutzmaßnahmen für Sie planen kann? Dafür müsste er so viel wissen, wie alle Mitarbeiter zusammen. Das wäre wohl zu viel verlangt.)

- **Geringe betriebliche Einbindung** (Der Datenschutzbeauftragte kann nicht überall präsent sein. Es bedarf aber ständiger Wachsamkeit! Wer denkt an den Datenschutz, wenn neue Produktideen aufkommen? Wer erkennt ein Problem, wenn es plötzlich auftritt? Das können nur die Mitarbeiter am Ort des Geschehens sein. Doch wie schafft man es, dass die Mitarbeiter WIRKLICH sensibilisiert sind? Ganz sicher nicht durch Schulungen und Newsletter. Nein, die Mitarbeiter müssen den Datenschutz VERSTEHEN und irgendwann selbst im Blut haben. Deswegen kann man nicht alles Knowhow und alle Arbeiten auf den Datenschutzbeauftragten schieben.)

- **Datenschutz ist Teamarbeit** (Viele Vorgänge im Datenschutz lassen sich nur dann verlässlich und zeitnah erfüllen, wenn das Unternehmen als „Team“ agiert. Probleme wären programmiert, wenn jede Abteilung mit Tunnelblick vor sich hin arbeitet. Doch wie sollten sich Teams herausbilden, wenn alle denken: „Der Datenschutzbeauftragter wird es schon richten“?)

Fazit: Es geht kein Weg drumherum: Die Plan-Do-Check-Act-Zyklen müssen durch Ihre eigenen Mitarbeiter erarbeitet und mit Leben erfüllt werden. Der Datenschutzbeauftragte ist mit der diesbezüglichen Unterrichtung, Beratung und Überwachung (mehr als) genügend beschäftigt. Siehe Kapitel 11 ab Seite 221.

13.3 Fachliteratur und Informationsquellen

Fachinformationen

Die betriebliche Umsetzung der DS-GVO liegt zu großen Teilen bei den Mitarbeitern der Unternehmen. Zur Erarbeitung des betrieblichen Knowhows ist die Nutzung von Fachliteratur unumgänglich. Wo finden Sie das entsprechende Knowhow?

13.3.1 Onlinezugang zum Verordnungstext

Wo kann man schnell und unbürokratisch auf die Texte der DS-GVO und des BDSG-neu zugreifen?

➔ In der Einleitung auf Seite 10 nennen wir Ihnen die Online-Quellen.

Die für den Datenschutz zuständigen Mitarbeiter sollten die obigen Webseiten unbedingt als Bookmark in die Favoritenleiste ihres Webbrowsers legen, um jederzeit schnell auf den Verordnungstext zugreifen zu können.

a) Fehler im Text der DS-GVO

Derzeit sind uns die folgenden **10 wesentlichen Fehler** in der deutschen Fassung der DS-GVO bekannt (siehe auch hier):

- Artikel 14 (1) muss mit „Wurden“ beginnen, nicht mit „Werden“
- Artikel 15 (4) muss auf Absatz 3 verweisen, nicht auf 1b
- Artikel 20 (4) muss sich auf Absatz 1 beziehen, nicht auf 2
- Artikel 28 (7) muss sich auf Artikel 93 (2) beziehen, nicht auf Artikel 87 (2)
- Artikel 30 (5) wurde komplett umformuliert mit völlig anderer Aussage
- Artikel 33 (1) muss sich auf Artikel 55 beziehen, nicht auf 51
- Artikel 37 (3) muss „ernennen“ statt „benennen“ heißen
- Artikel 62 (2) muss sich auf Absatz 5 beziehen, nicht auf Absatz 4
- Artikel 83 (1) muss sich auch auf den Absatz 4 beziehen, nicht nur auf die Absätze 5 und 6
- Artikel 83 (2) muss sich auf das Literal j beziehen und nicht auf i

Bitte beachten Sie diese Fehler unbedingt, sofern Sie auf die EU-Originaltexte zugreifen wollen oder sich den Verordnungstext auf anderen Websites anschauen möchten.

13.3.2 Kommentare

Die folgenden Werke vermitteln einen intensiven Einstieg und kommentieren jeden einzelnen Verordnungs-Artikel.

Die für den Datenschutz zuständigen Mitarbeiter sollten mindestens auf einen Kommentar zugreifen können. Lassen Sie sich von den dicken Büchern nicht abschrecken! Die Kommentare sind sehr systematisch aufgebaut, sodass man in weniger als einer Minute zu den gewünschten Kommentierungen findet. Ohne jeden Fachkommentar bleibt die DS-GVO unverständlich und unanwendbar.

- „**Datenschutzrecht**“, Bergmann/Möhrle/Herb
  Ca. 3.600 Seiten, 96 € (für ein Jahr)
  Die Ergänzungslieferung von September 2016 hat die Artikel 1, 30 und 32 kommentiert.
  Mit jeder weiteren Ergänzungslieferung werden wohl neue Artikel hinzukommen.
- „**DSGVO / BDSG**“, Eßer/Kramer/von Lewinski
  Ca. 2.000 Seiten, 149 € (~September 2017)
- „**BDSG / DSGVO**“, Plath
  ca. 1.700 Seiten, 139 €
- „**Europäische Datenschutzgrundverordnung**“, Sydow, ca. 1.500 Seiten, 128 €
- „**Datenschutz-Grundverordnung: DS-GVO**“, Ehrmann/Selmayr
  Ca. 1.350 Seiten, 138 €
- „**Datenschutz-Grundverordnung: DS-GVO**“, Kühling/Buchner
  Ca. 1.200 Seiten, 159 €.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

13.4 Informations-Sicherheits-Managementsysteme

Fachinformationen

Wie kann man die Informationssicherheit dauerhaft gewährleisten?

Es sind technische und organisatorische Maßnahmen zu treffen, um eine sichere Datenverarbeitung gemäß Artikel 32 (1) dauerhaft sicherzustellen. Dabei muss das Risiko der jeweiligen Datenverarbeitung angemessen berücksichtigt werden. Nur ein „Informations-Sicherheits-Managementsystem“ (ISMS) kann all dies gewährleisten.

➔ Siehe [Pflicht_032] auf Seite 124.

➔ Ein beispielhaftes Formular zur Auswahl eines ISMS findet sich im Kapitel 12.14 auf Seite 265.

Die folgenden Unterkapiteln sollen einen Überblick verschaffen: Welche Arten von ISMS gibt es am Markt? Wie aufwändig sind sie? Was kosten sie?

13.4.1 Technisch-organisatorische Maßnahmen auflisten

Nur der Vollständigkeit halber sei diese Auflistung der TOMs hier aufgeführt. Natürlich sind solche Listen kein ISMS. Ein geschlossener Nachweis einer Informations-Sicherheits-Strategie fehlt völlig. Trotzdem ist eine solche Maßnahmen-Liste besser als nichts.

- Ultrakurz-Checkliste
  Manche Verantwortliche werden den Aufwand auf das absolute Minimum reduzieren wollen. Hierfür steht eine entsprechende Checkliste im Kapitel 12.15.2 auf Seite 280 zur Verfügung.

- Kurz-Checkliste der VdS
  In dem Anforderungskatalog der VdS-3473 (siehe unten) findet man in den Kapiteln 4 („Organisation der Informationssicherheit“) bis 18 („Sicherheitsvorfälle“) insgesamt 15 gute Überschriften, um sich selbst Gedanken über die IT-Sicherheits-Organisation zu machen. Das ist eine sehr gute Grundlage für ein ausführliches IT-Sicherheits-Konzept.

13.4.2 Minimallösungen basierend auf Fragebögen

Die folgenden Fragebögen sind kein ISMS, aber immerhin kann ein Unternehmen nachweisen, dass es sich systematisch mit Fragen der IT-Sicherheit auseinandergesetzt hat. Diesen Level darf man erwarten von kleinen Dienstleistern mit 1-5 Mitarbeitern. Wenn es also darum geht, solche Dienstleister als Auftragsdatenverarbeiter im Sinne Artikel 28 DS-GVO einzusetzen, sollte man mindestens einen solchen Nachweis fordern (siehe Pflicht [GVO_028] auf Seite 159).

- ISA⁺ - Informations-Sicherheits-Analyse (noch nicht zertifizierbar)
  Mit diesem Fragenkatalog werden die 50 wichtigsten Aspekte der IT-Sicherheit abgefragt (kostenlos bestellbar bei felix.struve@it-sec-cluster.de). Es stehen erfahrene Berater zur Verfügung, die beim Ausfüllen helfen können. Eine Zertifizierung ist geplant, aber im Juni 2016 noch nicht verfügbar. [56]

  Auf Nachfrage war zu erfahren, dass im Jahr 2017 die ersten beiden Zertifizierungen geplant sind. Die DQS GmbH wird dies durchführen (die Kosten sollten 2.000 € nicht übersteigen.)
  (Der Dienstleister PSW sieht diesen Ansatz als geeignet für Unternehmen bis 50 Arbeitsplätze. Für einen Pauschalpreis von unter 1000 € wird der ausgefüllte Bogen geprüft (Stand 2016). Der Aufwand bei Begleitung bis zu einer (zukünftigen) Zertifizierung liegt bei mindestens zwei Manntagen.)

[56] Interessant ist der 91-seitige BSI-„Leitfaden Informationssicherheit“, der vieles Grundlegende erklärt. Dort im Anhang im Kapitel 10.1 befinden sich Checklisten, die den ISA⁺-Fragen ähneln.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

13.5 Weitergabe von Daten – ein Merkblatt

Fachinformationen

Welche rechtlichen Möglichkeiten gibt es, wenn ein Verantwortlicher seine personenbezogenen Daten mit anderen Unternehmen „teilen“ möchte?

Die DS-GVO liefert kein geschlossenes Bild davon, wie die **Weitergabe von Daten** an Empfänger außerhalb des eigenen Unternehmens zu gestalten ist. Die Fachliteratur geht auf diese Frage bisher leider nicht ausreichend präzise ein.

ACHTUNG: Das „Merkblatt zur Weitergabe von Daten“ stellt lediglich einen **Versuch** dar, das begriffliche Gewirr der DS-GVO zu klären. Die Umstände rund um **(a)** die Offenlegung von Daten an Empfänger und **(b)** der gemeinsame Zugriff mit anderen Verantwortlichen und **(c)** die Veröffentlichung von Daten im Internet und Registern ist EXTREM komplex. Die DS-GVO unternimmt keinerlei Anstrengungen, um hier ein Gesamtkonzept oder auch nur Definitionen zu liefern. Hinzu kommen systematische Schwierigkeiten in der deutschen Übersetzung. Insofern ist das Ergebnis dieses Merkblatts **unverbindlich.**

Die folgenden Kapiteln sind alle identisch aufgebaut: Wir nennen die Definitionen, zeigen die Textstellen, nennen formelle Voraussetzungen, zeigen rechtliche Zulässigkeiten auf, erläutern die Haftungsfrage und nennen die dazugehörige Pflicht im PrivazyPlan®. Ganz bewusst halten wir uns hier so kurz und knapp wie möglich, damit das Gesamtbild nicht vor lauter Details verloren geht.

13.5.1 Offenlegung an „Empfänger“

Ein Empfänger im Sinne des Artikel 4 Nr. 9 ist „*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten* ***offengelegt*** *werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht*“.

Es handelt sich also um eine gezielte Offenlegung von personenbezogenen Daten an einen konkreten Adressaten außerhalb des eigenen Unternehmens. Die wichtigsten Textstellen hierzu finden sich im Dossier „Offenlegung“. Hier können drei Unterfälle unterschieden werden:

a) Übermittlung an Dritte innerhalb der EU und des EWR

Dieses Szenario der „Übermittlung“ wird in der DS-GVO leider nicht explizit definiert oder beschrieben. Es hat den Anschein, dass die Übermittlung gemäß Artikel 4 Nr. 2 ein ganz normaler Verarbeitungsvorgang ist: „*Verarbeiten ist […] die Offenlegung durch Übermittlung*“. Mehr nicht.

Die Empfänger sind „Dritte“ gemäß Artikel 4 Nr. 10: „*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle […]*“. Gemeint ist also grob gesagt Jeder außerhalb des eigenen Unternehmens. (Ausnahme: Behörden mit Untersuchungsauftrag gemäß Erwägungsgrund 31.)

Die Ähnlichkeit zum § 3 Abs. 4 Nr. 3 BDSG (gültig in Deutschland bis zum 25.05.2018) ist offensichtlich.

Die „Übermittlung“ ist ein alltäglicher Vorgang im Unternehmen. Hierunter fällt beispielsweise die gesetzlich geforderte Übertragung von Beschäftigtendaten an die Krankenkasse.

Die wichtigsten **Textstellen** hierzu finden sich im Dossier „Übermittlung“. Der englische Originaltext verwendet dort den Begriff „transmit“ bzw. „transmission“. Dies wurde in der deutschen Übersetzung durchweg als „Übermittlung“ übersetzt (leider genauso wie das englische „transfer“ in Bezug auf die Übermittlung

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

13.6 Risikomatrix anwenden

Fachinformationen

Die Quantifizierung von Risiken ist eine schwierige Angelegenheit. Die Fachliteratur erwähnt oftmals die „Risikomatrix“. Was steckt dahinter?

In der DS-GVO spielt der Begriff „Risiko“ eine große Rolle (siehe Kapitel 6.1 ab Seite 142). Leider ist die objektive Einschätzung eines Risikos eine schwierige Angelegenheit, weil mit vielen unbestimmten Begriffen gearbeitet werden muss.

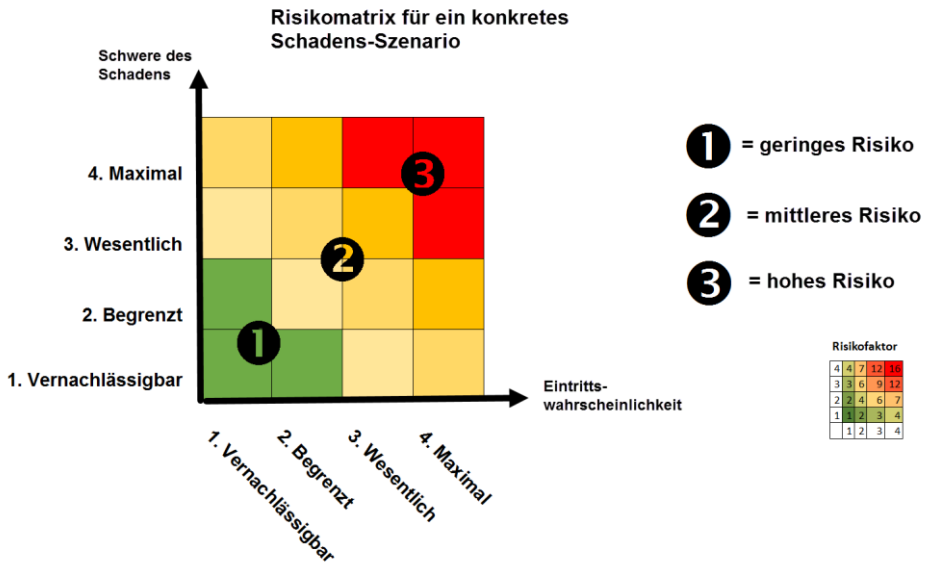
Die Risikoeinschätzung spielt unter anderem eine wichtige Rolle

- in der DS-GVO beim Artikel 33 (1) bezüglich der Meldung einer Datenschutzverletzung an die Aufsichtsbehörde (bei einem mittleren oder hohen Risiko). Ebenso im Artikel 34 (1) bezüglich der Meldung einer Datenschutzverletzung an die betroffene Person (bei einem hohen Risiko).
  Siehe Pflicht [GVO_033a] auf Seite 135.
- in der DS-GVO im Artikel 35 (1) bezüglich der Folgenabschätzung einer Verarbeitung, sofern die Verarbeitung voraussichtlich ein hohes Risiko in sich birgt.
  Siehe Pflicht [GVO_035] Seite 142.
- für den Datenschutzbeauftragten, der gemäß Artikel 39 (2) risikoorientiert tätig werden soll.
- in der IT-Sicherheit, wenn das Risiko von IT-Systemen abgeschätzt werden soll. Jedes IT-Sicherheits-Management-System (ISMS) arbeitet mit Risikoabschätzungen, um das Maß der Sicherheitsmaßnahmen abschätzen zu können. Siehe Seite 316.

Viele Fachleute schlagen eine Risikomatrix vor, in welcher für ein konkretes Schadensszenario die Klassifizierung nach „Eintrittswahrscheinlichkeit“ und „Schwere des Schadens“ vorgenommen wird.

In jedem der obigen vier Beispiele unterscheiden sich (a) die Art des Risikos, (b) die Risiko-Szenarien, (c) die Wahrscheinlichkeitskriterien, (d) die Schadensart, (e) die möglichen Gegenmaßnahmen. Aus diesem Grund kann die Anwendung der Risikomatrix hier nur in allgemeiner Form beschrieben werden.

Die folgende Abbildung zeigt eine typische Risikomatrix:



Solch eine Risikomatrix macht natürlich nur dann Sinn, wenn die zugrundeliegenden Bestandteile nachvollziehbar und ausführlich charakterisiert werden. Auf diese Problemstellung gehen die meisten Autoren leider nicht ein (vielleicht weil das die scheinbare Einfachheit der Risikomatrix schnell verkomplizieren würde).

So gesehen liegt das „eigentliche Knowhow“ nicht in der obigen simplen Tabelle, sondern darin, wie man sie korrekt anwendet. Genau das wird im Folgenden beschrieben.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 360; eine tabellarische Übersicht auf Seite 377.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 232.

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 205) werden alle Pflichten des Verantwortlichen ausführlich beschrieben und angeleitet.

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 274). ● 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.

... die restlichen Kurzzusammenfassungen finden Sie in der Vollversion…

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

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)	30
2.2	xxx [GVO_013a]	Artikel 13 (3)	34
2.3	xxx [GVO_014]	Artikel 14	38
2.4	xxx [GVO_015]	Artikel 15 (1,2)	43
2.5	xxx [GVO_015a]	Artikel 15 (3,4)	46
2.6	xxx [GVO_016]	Artikel 16	50
2.7	xxx [GVO_017]	Artikel 17 (1)	52
2.8	xxx [GVO_017a]	Artikel 17 (1)	55
2.9	xxx [GVO_017b]	Artikel 17 (2)	57
2.10	xxx [GVO_018]	Artikel 18	60
2.11	xxx [GVO_019]	Artikel 19	64
2.12	xxx [GVO_020]	Artikel 20	68
2.13	xxx [GVO_021]	Artikel 21	72
2.14	xxx [GVO_022]	Artikel 22	76

Pflichten zu Dokumentationen und Nachweisen

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

3.1	Nachweis der Einhaltung der „Grundsätze“ [GVO_005]	Artikel 5 (2)	80
3.2	xxx [GVO_025]	Artikel 25	87
3.3	xxx [GVO_030]	Artikel 30 (1)	90
3.4	xxx [GVO_030a]	Artikel 30 (2)	95

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)	100
4.2	xxx [GVO_006a]	Artikel 6 (4)	107
4.3	xxx [GVO_007]	Artikel 7 (1)	111
4.4	xxx [GVO_007a]	Artikel 7 (2)	114
4.5	xxx [GVO_007b]	Artikel 7 (3)	116
4.6	xxx [GVO_007c]	Artikel 7 (4)	118
4.7	xxx [GVO_008]	Artikel 8 (2)	121

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)	124
5.2	xxx [GVO_032a]	Artikel 32 (4)	128
5.3	xxx [GVO_033]	Artikel 33 (5)	132
5.4	xxx [GVO_033a]	Artikel 33 (1)	135
5.4	xxx [GVO_034]	Artikel 34 (1)	138

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	142
6.2	xxx [GVO_036]	Artikel 36	147

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	150
7.2	xxx [GVO_027]	Artikel 27	156
7.3	xxx [GVO_028]	Artikel 28	159
7.4	xxx [GVO_028a]	Artikel 28 (3a)	164
7.5	xxx [GVO_028b]	Artikel 28 (3)	170
7.6	xxx [GVO_044]	Artikel 44	172

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)	177
8.2	xxx [GVO_037a]	Artikel 37 (7)	182
8.3	xxx [GVO_038]	Artikel 38 (1)	185
8.4	xxx [GVO_038a]	Artikel 38 (2)	188
8.5	xxx [GVO_038b]	Artikel 38 (4)	190
8.6	xxx [GVO_039]	Artikel 39 (1a)	192
8.7	xxx [GVO_039a]	Artikel 39 (1b)	195
8.8	xxx [GVO_039b]	Artikel 39 (1e)	198

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) Pflichten eines Website-Diensteanbieters [TMG_013]	§ 13 TMG	203
9.4.3	b) Berufliche Schweigepflicht [STGB_203]	§ 203 StGB	204
9.4.3	c) Unzumutbare Werbe-Belästigungen [UWG_007]	§ 7 UWG	204

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	Videoüberwachung kenntlich machen [BDSG_004]	§ 4 Abs. 2	206
10.2	xxx [BDSG_004a]	§ 4 Abs. 4	209
10.3	xxx [BDSG_022]	§ 22 Abs. 2	211
10.4	xxx [BDSG_027]	§ 27 Abs. 3	213
10.5	xxx [BDSG_030]	§ 30 Abs. 1	214
10.6	xxx [BDSG_030a]	§ 30 Abs. 2	215
10.7	xxx [BDSG_035]	§ 35 Abs. 2	216

14.4 Unsichere Sachverhalte (rote Bomben)

Anhang

Bezüglich des EU-weiten Datenschutzes ab dem 25.05.2018 gibt 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)

💣 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. (Seite 12)

💣 Zählt auch eine heimliche Erhebung von personenbezogenen Daten als eine Dritt-Erhebung im Sinne des Artikel 14? Bezieht sich also die Dritterhebung auch auf Daten, die der Verantwortliche zwar selbst erhebt, ohne dass aber die Person aktiv tätig wird? Wenn es also heimlich bzw. verdeckt geschieht? Dies wird bezüglich einer heimlichen Videoüberwachung gemäß Gola-Fachkommentar in RdNr. 2 zu Artikel 14 so interpretiert. Ebenso im Kühling/Buchner-Fachkommentar in RdNr. 21 zu Artikel 14 im Falle von statistischen Auswertungen vom Surfverhalten einer Person. Bis sich diese (etwas überraschende) Interpretation erhärtet geht der PrivazyPlan® erstmal nicht davon aus, dass dies so stimmt. In den folgenden Ausführungen wird angenommen, dass es allein um die Datenerhebung durch Dritte geht. (Seite 38)

💣 Wenn die betroffene Person ihre Daten **selbst per Software** berichtigt/löscht/einschränkt: Ist das als ein entsprechendes „Verlangen“ gemäß Artikel 19 zu interpretieren, wonach der Verantwortliche eine „Nachberichtigung“ durchführen muss? Die Fachliteratur geht darauf nicht ein. Einerseits wäre das sehr weit interpretiert und hätte enorme Auswirkungen (weil dann sehr oft nachberichtigt werden müsste). Andererseits: Warum sollte man die Onlinenutzer benachteiligen? Im August 2017 ist diese Fragestellung noch völlig offen. (Seite 66)

💣 Wann liegt eine **unzulässige Kopplung** von Einwilligung und Vertragserfüllung gemäß Artikel 7 (4) vor? Die Aufsichtsbehörden und Gerichte werden im Laufe der Zeit entsprechende Hürden formulieren. Bis dahin steht zu befürchten, dass Beschwerden und Abmahnungen drohen könnten. (Seite 119)

… die restlichen roten Bomben finden Sie in der Vollversion.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ
AUF KURS.

... dies ist einen Leseprobe.

Wenn Sie die Vollversion des PrivazyPlan® lizenzieren wollen,
so besuchen Sie uns auf
www.privazyplan.eu

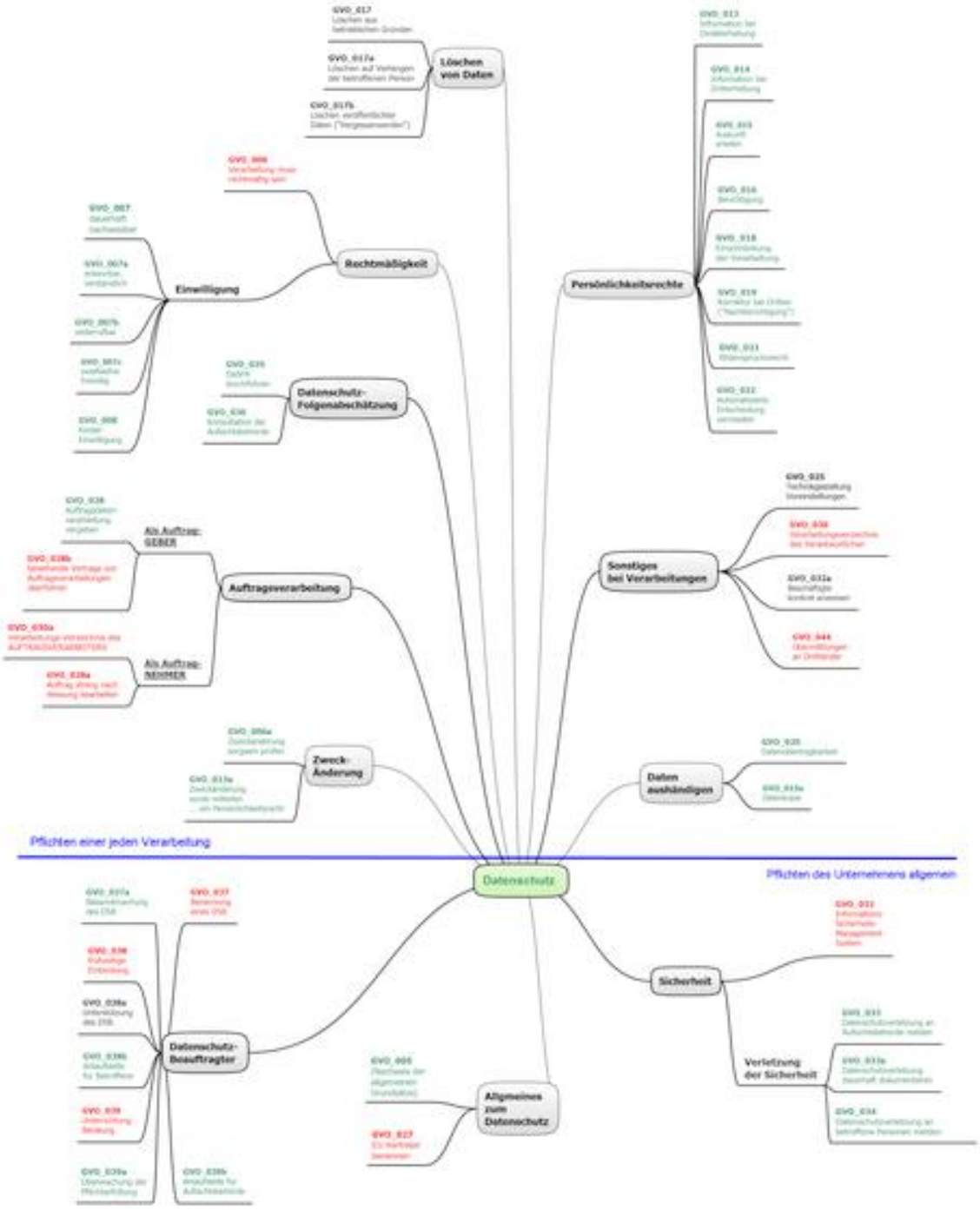
14.5 Mindmap der Pflichten

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-neu 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.

...

A

B

C

D

E

F

G

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z