PRIVAZYPLAN®

Praxisleitfaden für Datenschutz.

Herzlich willkommen in der Leseprobe des PrivazyPlan®
in der Ausgabe Mai 2022.
Hier zwei kleine Tipps: Mit ALT+Linkspfeil gelangen Sie
zurück zur Hyperlink-Sprungstelle. Externe Hyperlinks
öffnen Sie mit STRG+Mausklick, um einen neuen Tab zu öffnen.

Diese Leseprobe zeigt 166 von 705 Seiten.

PRIVAZYPLAN®

BRINGT IHREN DATENSCHUTZ AUF KURS.

von
SecureDataService
Nicholas Vollmer

im Mai 2022

Zertifizierter Datenschutz gemäß der VdS-Richtlinie 10010.
Unser betriebliches Datenschutz-Managementsystem erfüllt strengste Anforderungen.
Das zweitägige Vor-Ort-Audit bei SecureDataService beweist:
Der **PrivazyPlan®** als Praxisleitfaden funktioniert!
Siehe Seite 512.

Inhaltsverzeichnis

… ein ausführliches Inhaltsverzeichnis finden Sie auf Seite 686.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checkliste des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

1.1 Vorwort zur aktuellen Ausgabe

Einleitung

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen zur aktuellen Ausgabe im Mai 2022. An **23 Stellen** wurden kleinere Aktualisierungen vorgenommen.
Der Gesamtumfang des PrivazyPlan® (inkl. aller zusätzlichen Dokumente in der Privazyplan.zip) beträgt derzeit 705+321=1.026 Seiten.

Diesen Monat gibt es ausnahmsweise keine wesentlichen Neuerungen. Das ist eigentlich eine positive Nachricht, denn das bedeutet auch, dass die Datenschutzwelt nicht komplizierter geworden ist. ;-)

Erleben Sie alle wichtigen Kapitel mittels einer geführten Tour auf Seite 697 .

Ich wünsche Ihnen ein gutes Gelingen im Datenschutz…

P.S. Wenn Sie wirklich **alle** Stellen finden wollen (also auch die nicht so Wichtigen) dann suchen Sie z.B. nach dem Text „Neu im Mail“. Außerdem gibt es neue Fachliteratur; suchen Sie nach „Neue Literatur“, um diese Stellen zu finden.

1.2 Allgemeines Vorwort (im Mai 2022)

Einleitung

Liebe Leser,

als Autor des PrivazyPlan® heiße ich Sie herzlich willkommen.

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

Die Zeit vergeht wie im Flug. Im Januar **2011** präsentierte die EU-Vizepräsidentin (Frau Viviane Reding) in Brüssel den Kommissions-Entwurf einer Datenschutz-Grundverordnung. Im April **2016** hat Europa sich (völlig überraschend) ein neues Datenschutzrecht erschaffen, welches seit Mai **2018** anzuwenden ist.

… nun sind wir im Mai 2022 und die DS-GVO hat die ersten sechs Jahre hinter sich gebracht. Wie ist der Stand der Dinge?

Die gute Nachricht ist: Die große **Datenschutz-Katastrophe ist ausgeblieben**. Die Datenschutz-Aufsichtsbehörden haben bisher (fast) keine exorbitanten Bußgelder verhängt, und auch die befürchteten Massen-Abmahnungen sind ausgeblieben. Das Recht auf immateriellen Schadenersatz spielt kaum eine Rolle und wurde nur selten missbraucht.

Die vielleicht größte Hoffnung der DS-GVO wurde nicht erfüllt: Die **US-amerikanischen Anbieter** wurden zwar dem EU-Recht unterworfen, doch war dies de facto wirkungslos. Die irische Aufsichtsbehörde blockiert die Verfahren wie zu Zeiten vor der DS-GVO. Die sagenhaften Bußgelder von bis zu 4% vom weltweiten Umsatz wurden nicht verhängt. Dieses Unrecht geht zulasten der EU-Softwareindustrie (siehe „Digitale Souveränität für Europa“ ab Seite 660).

Insofern ist die **Baustelle der weltweiten Datentransfers** aus unserer Sicht nach wie vor das größte Problem für die meisten europäische Unternehmen (siehe Seite 222). Weder die Websitegestaltung, noch weitere Schritte der Digitalisierung sind ohne US-Dienste denkbar... das zeigt die tägliche praktische Erfahrung. Die europäische Software-Industrie bietet (fast) keine Alternativen (oder nutzt im Hintergrund ebenfalls US-Rechenzentren).

Die angekündigte **ePrivacy-Verordnung** lässt noch immer auf sich warten, wodurch viele wichtige Fragen des Internets ungeklärt bleiben (siehe Seite 262).

Leider hat die allgemeine **Rechtsunsicherheit** zugenommen (siehe Seite 692), und viele wichtige Themen sind strittig. Die deutschen Aufsichtsbehörden verkomplizieren die Lage durch uneinheitliche Bewertungen und ständig neue Auflagen. Die vielen (oft widersprüchlichen) Gerichtsentscheidungen sind in der Praxis oftmals keine Hilfe.

Die **Komplexität** des Datenschutzes steigt kontinuierlich an. Als Autor des PrivazyPlan® wird es zusehends schwieriger einen konsistenten **Praxis**leitfaden aufrecht zu erhalten. Mittlerweile bedarf es wöchentlich mehrerer Stunden, um auf dem aktuellen Stand der Dinge zu bleiben und praxisgerecht zu berichten. Nicht ohne Grund nimmt der Umfang des PrivazyPlan® um derzeit 100 Seiten jährlich zu.

Nicht ohne Stolz möchte ich darauf hinweisen, dass mein Unternehmen SecureDataService seit August 2020 gemäß der VdS-Richtlinie 10010 über ein zertifiziertes Datenschutz-Managementsystem verfügt (siehe Seite 512); als eines von wenigen Unternehmen bundesweit. Davon haben die Leser des PrivazyPlan® enorm profitiert.

Seien Sie versichert: Ich bleibe für Sie am Ball. Mein Ehrgeiz für einen (tages-) aktuellen Praxisleitfaden ist ungebrochen. Der PrivazyPlan® bleibt Ihr verlässlicher Lotse im schwierigen Fahrwasser des Datenschutzes.

Und nun, im Mai 2022, wünsche ich Ihnen eine angenehme Lektüre und ein gutes Gelingen!

Nicholas 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 Februar: …“ und „Zurück zum Vorwort“.
  - Kleine Änderungen werden komplett eingefärbt und sehen dann folgendermaßen aus: „Neu im Februar: 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.

1.3.2 Navigationshilfen im PDF-Dokument

Station 1: Navigation im PrivazyPlan®

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

< Zurück • Home • Weiter >

Der PrivazyPlan® ist mit über 600 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 entspre-

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 502 (mit einer Kurzzusammenfassung auf Seite 511).

Den idealen Einstiegspunkt in die DS-GVO und den PrivazyPlan® erhalten Sie übrigens auf Seite 310.

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 404
- die Kurzzusammenfassung aller Pflichten ab Seite 674
- das ausführliche Inhaltsverzeichnis ab Seite 686
- die tabellarische Übersicht aller Pflichten ab Seite 689
- den Index ab Seite 700

… und legen Sie sich diese Ausdrucke griffbereit zur Seite.

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

1.4.2 Den Datenschutz überblicken (Schritt 2)

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

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

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

a) Die Datenschutz-Grundverordnung (DS-GVO)

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

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

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

Ganz besonders stolz sind wir auf die „**Dossier**“-Funktion auf http://www.privacy-regulation.eu/de/j8e5w/dossier_compliance.htm. 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)

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

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

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

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

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

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

1.4.3 Ausrichtung nach Pflichten (Schritt 3)

Worum geht es den meisten Unternehmen, wenn sie den Datenschutz einhalten wollen? Sie wollen **Geldbußen vermeiden** (siehe Seite 575). Daher zerlegt der PrivazyPlan® die DS-GVO (inkl. des neuen Bundesdatenschutzgesetzes) in die diesbezüglichen Pflichten.

a) Was sind Pflichten? Wo findet man sie?

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

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

Generell sollten alle **relevanten Geldbußen-Bestimmungen** des Artikel 83 (4) und Artikel 83 (5) als „Pflichten“ gelten. Darauf basierend haben wir alle konkret fassbaren Pflichten gesucht, die sich an Formulierungen erkennen lassen wie „… *hat sicherzustellen…*“ oder „… *hat zu dokumentieren…*“. [3]

Auf Seite 575 finden Sie weitergehende Informationen zu Geldbußen, Schadenersatz, Interventionsmöglichkeiten der Aufsichtsbehörden etc.

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

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

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

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

---

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

Durch das zweitägige Vorort-Audit bei SecureDataService zur VdS-Richtlinie 10010 können wir im Oktober 2020 sagen: JA, der Pflichten-Ansatz des PrivazyPlan® hat sich bewährt! Siehe Seite 512.

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. [4]
  In Deutschland steht ein „BDSG“ für das neue Bundesdatenschutzgesetz.

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

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

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

c) Und was ist mit den möglichen Schadenersatzforderungen?

Unabhängig von den Geldbußen drohen natürlich auch Schadenersatzforderungen. Die betroffenen Personen können gemäß Artikel 82 sowohl materielle als auch immaterielle Schäden geltend machen (siehe Seite 582).
Doch lassen sich potenzielle Schadenersatzforderungen im Verordnungstext noch schwieriger eingrenzen als Geldbußen-Gefahren. Im Prinzip kann eine betroffene Person durch „beliebige“ Sachverhalte einen Schadenersatz geltend machen.
Da dies kaum einzugrenzen ist, konzentriert sich der PrivazyPlan® zunächst einmal nur auf die Gefahren von Geldbußen.

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

1.4.4 Pflichten verständlich machen (Schritt 4)

Jede einzelne Pflicht erklären wir ganz konkret. Sie erfahren:

- worin die Pflicht besteht (in wenigen Sätzen zusammengefasst),
- ob das Bundesdatenschutzgesetz ähnliche Pflichten kannte,
- wo die dazugehörige Bestimmung zur Geldbuße zu finden ist (siehe auch Seite 575),
- ob es konkrete Fachliteratur gibt,
- ob in Deutschland das neue Bundesdatenschutzgesetz hier Anwendung findet,

[Ab hier eine Lücke aufgrund der Leseprobe...]

[4] Für die Pflichten des Datenschutzbeauftragten lauten die Kürzel „[DSB_...]“, siehe Kapitel 11 ab Seite 264.

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

In Deutschland gilt gemäß § 38 BDSG u.a. eine Benennungspflicht, wenn mindestens **zehn Personen** ständig mit der automatisierten Datenverarbeitung beschäftigt sind (also z.B. über persönliche E-Mail-Adresse verfügen). Siehe Seite 236.

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

1.5 Wichtige Entscheidungen vorab

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

Die Ergebnisse Ihrer Überlegungen können Sie beispielsweise in der **Datenschutz-Leitlinie** hinterlegen (siehe Seite 326).

1.5.1 Welches Compliance-Managementsystem passt zu Ihnen?

Bekanntlich ist der Datenschutz ein **Compliance**-Thema (siehe Seite 502).

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 502.

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?

[Ab hier eine Lücke aufgrund der Leseprobe...]

1.6 Priorisierung der Pflichten

Einleitung

Im Rahmen von PrivazyPlan® werden ca. 50 Pflichten identifiziert. Die Priorisierung sollte möglichst frühzeitig in Angriff genommen werden. Falls Sie einen Datenschutzbeauftragten benannt haben, so wird er Sie sicherlich unterstützen (siehe Seite 299).

Übrigens liefert das DSK-Kurzpapier-8 auch einen allgemeinen „Maßnahmenplan“.

[Wird Ihr Unternehmen durch einen Datenschutzbeauftragten betreut, der im Rahmen von DSB-MIT-SYSTEM® tätig ist? Dann kann er Ihnen das Dokument DOC_073 („ds_aktionsplan.doc“) zur Verfügung stellen. Hier werden alle wichtigen Belange grob thematisiert.]

1.6.1 Ein grober Plan zur Umsetzung der DS-GVO

Bevor Sie mit den folgenden Punkten beginnen, so sei vorausgesetzt, dass Sie die grobe Einleitung auf Seite 310 gelesen haben.

In vier Tagen können Sie die Umsetzung der DS-GVO **anstoßen**. Das Ergebnis eines jeden Tages ist die Benennung einer konkreten Person, die sich den geforderten Aufgaben widmet (im Folgenden rot markiert). Die VdS-Richtlinie 10010 (Seite 512) vertieft diese Aspekte im dortigen Kapitel 4 („Organisation“).

Die 23-seitige GDD-Praxishilfe DS-GVO II („Verantwortlichkeiten und Aufgaben“) – stark überarbeitet im August 2021 - kann ebenfalls hilfreich sein, um die Verantwortlichkeiten und Zuständigkeiten zu organisieren.

a) Tag 1: Die Geschäftsführung nimmt die Herausforderung an

Die Umsetzung der DS-GVO steht und fällt mit der Entschlossenheit der Geschäftsführung. Nur wenn die Geschäftsführung die Prioritäten setzt und die

[Ab hier eine Lücke aufgrund der Leseprobe...]

1.7 Allgemeine Bearbeitungshinweise (zum PDCA-Zyklus)

Einleitung

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

Da bekanntlich ein **Compliance-Managementsystem (CMS)** angestrebt wird (siehe Seite 502), ist jede Pflichterfüllung zunächst mittels „PLAN, DO, CHECK, ACT“ zu organisieren. Dies ist der bekannte PDCA-Zyklus.

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

In allen vier Phasen des PDCA-Zyklus werden Sie die Aufforderung finden, dass **ein neues Dokument erstellt** werden muss. Dies ist natürlich nur eine unverbindliche Empfehlung. Sie entscheiden selbst, wie Sie Ihr CMS organisieren: In MS-Word oder in einer spezialisierten Software oder in Form eines Ticket-Systems. Siehe die diesbezügliche generelle Überlegung auf Seite 593.

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

1.7.1 Allgemeine Planungshinweise („plan“)

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

a) Allgemeine Planungshinweise FÜR ALLE PFLICHTEN

Vorab: Möglicherweise gibt es eine inhaltliche Wechselwirkung mit der „Datenschutz-Leitlinie“, die die Geschäftsleitung formuliert und unterschreibt (siehe Seite 326, und zwar speziell im Unterkapitel „Operative Umsetzung“). In jener Leitlinie werden eventuell schon ganz grobe Planungsschritte vorweggenommen. Alles, was in der Leitlinie bereits formuliert ist, muss hier bei den Planungen nicht wiederholt werden.

Bei der Formulierung der allgemeinen Planungshinweise empfiehlt sich eine knackige Formulierung. Länger als 10 Sätze sollte sie nicht sein. Nennen Sie möglichst noch keine konkreten Namen zuständiger Personen. Diese Planung soll lediglich die Beschäftigten grob anweisen.

Die folgenden Planungs-Überlegungen sind für alle ca. 50 Pflichten relevant:

☐ Erstellen Sie ein neues Text-Dokument (z.B. in MS-Word, oder in Ihrem ggf. vorhandenen Dokumenten-Managementsystem) und nennen Sie es (sinngemäß) „*GVO_XXX_plan.docx*“. Hier können Sie alle Planungen dokumentieren.

[Hinweis: Das rote „GVO_XXX“ ist ein Platzhalter für das Kürzel der jeweiligen Pflicht. Es könnte „GVO_013“ lauten oder „STGB_203“ etc.]
Alternativ können Sie auch das „Simpel-Datenschutz-Managementsystem“ im Rahmen der Datei **PrivazyPlan.zip** nutzen (siehe Seite 29) und die Planungen im jeweiligen Tabellenblatt der MS-Excel-Tabelle dokumentieren.

Im Folgenden finden Sie einen beispielhaften Planungstext für die Pflicht „**Bei Erhebung von Daten ausführlich informieren [GVO_013]**“, siehe Seite 40.

„Für diese Pflicht gilt die Datenschutz-Richtlinie als Grundlage. Die Informationstexte sind frühzeitig zu erstellen und zentral abzuspeichern. Die im PrivazyPlan® beschriebenen Kürzel sollen verwendet werden. Die Texte sind stets aktuell zu halten; alte Versionen werden in einem Archiv gespeichert. Sofern die Verarbeitungen Internet-relevant sind, so sollten sie auf der Internetpräsenz Jedermann zur Verfügung gestellt werden. Der Name des Datenschutzbeauftragten sollte in den Informationstexten genannt werden (sofern er damit einverstanden ist).“

[Ab hier eine Lücke aufgrund der Leseprobe...]

1.8 Systematische Kürzel für Einwilligungen und Infotexte

Einleitung

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

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

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

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

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

Diese Kürzel könnte man vielfältig verwenden:

- Man könnte sie als Kürzel in eckigen Klammern hinter die Textveröffentlichung hinzufügen („[E001a_de]“), wodurch sie auf dem jeweiligen Formular (oder Webseite) immer leicht zu identifizieren ist. Sollte dieses Kürzel fehlen, so könnten „Insider“ sofort erkennen, dass dies möglicherweise ein nicht-kontrollierter Text ist.
- In einem konkreten Einwilligungsnachweis gemäß Pflicht [GVO_007] auf Seite 142 müsste man nicht immer den vollen Wortlaut dokumentieren (und zwar in der jeweiligen Landessprache), sondern man bräuchte nur das Kürzel erwähnen. Sehr praktisch!
- Durch diesen systematischen Umgang kann man der Aufsichtsbehörde sehr effizient nachweisen, dass man die Thematik der Einwilligungen ernst nimmt. Diese Tatsache wird bei der Höhe einer potenziellen Geldbuße bestimmt positiv gewürdigt.
- Auf der Firmen-Website kann man den Einwilligungstext publizieren, indem man das Kürzel als Dateinamen nutzt (z.B. „**e001a_de.htm**“). Dies ist gemäß Erwägungsgrund 58 eine zulässige Maßnahme, um für Transparenz zu sorgen. Dies ist insbesondere dann eine gute Maßnahme, wenn die Einwilligungs-Modalitäten z.B. nicht auf eine Postkarte passen. Dies gilt natürlich nur für den Fall, dass die Adressaten absehbar Internet-affin sind.

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

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

Die Speicherung sollte an zentraler Stelle in einem Dokumenten-Managementsystem auf revisionssichere Weise erfolgen und für alle relevanten Kollegen zugreifbar sein (siehe Seite 594).

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

[Ab hier eine Lücke aufgrund der Leseprobe...]

1.9 Was leistet der PrivazyPlan® nicht?

Einleitung

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

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

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

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

Der PrivazyPlan® ist kein zertifizierbares Datenschutz-Managementsystem. Zwar werden die Datenschutz-Pflichten erklärt und mit Checklisten versehen, aber eine vollständige Anleitung zur innerbetrieblichen Organisation findet sich nicht. In dieser Hinsicht sei beispielsweise auf die VdS-Richtlinie 10010 hingewiesen (siehe Seite 512).

Doch wo finden Sie klassisches Fachwissen?

- Übergreifendes Fachwissen finden Sie im Kapitel 13 („Fachinformationen“) ab Seite 494.
- Umfangreiche Tipps zu Fachbüchern und Onlinequellen finden Sie ab Seite 518.

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

Einleitung

Station 3: Dokument-Vorlagen / Ergebnisse speichern

Wo findet man ausfüllbare MS-Word-Vorlagen? Und wo kann man die ausgefüllten Formulare und Checklisten abspeichern?
In einem Video (10 Minuten) zeigen wir Ihnen wie das geht. Bitte unbedingt anschauen!

< Zurück • Home • Weiter >

Sie möchten ein Datenschutz-Managementsystem („DSMS“) in Ihrem Unternehmen ganz konkret realisieren? Selbstverständlich gibt es dafür hochspezialisierte Softwareprodukte (wie beispielhaft auf Seite 508 beschrieben). [8] Aber es geht auch simpler:

➔ Unter
finden Sie unseren Minimal-Vorschlag.

➔ Unter

finden Sie die gleiche Verzeichnisstruktur, allerdings ohne die konkreten Vorlagen und Beispiele. Dies können Sie nutzen, um Ihre eigenen Arbeitsergebnisse zu speichern.

Mit diesem von uns vorgeschlagenen „Mini-DSMS“ können Sie alle Pflichten des PrivazyPlan® in die Praxis umsetzen. Sie benötigen lediglich ein Tabellenbear-

[8] Im Englischen verwendet man den Begriff **Privacy Information Management System** („PIMS“). Diesbezüglich ist eine internationale Standardisierung geplant; die ISO/IEC sieht ein Datenschutz-Managementsystem als Erweiterung des ISMS an (siehe Seite 149). Eine entsprechende Norm ISO/IEC 27552 ist in Arbeit (siehe Seite 423). Das Fachbuch „Privacy Impact Assessment“ thematisiert diesen Aspekt im Kapitel 2.4 (siehe Seite 172).

beitungsprogramm. Zusammen mit der VdS-Richtlinie 10010 (Seite 512) lässt sich die DS-GVO sehr gut in die Praxis umsetzen.

Unser Ansatz basiert auf drei grundlegenden Ideen:

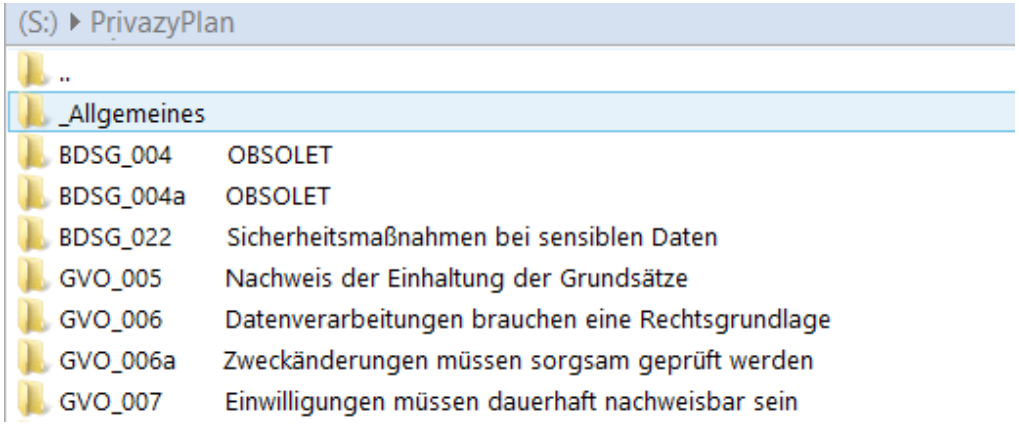
1. Für jede Pflicht des PrivazyPlan® wird ein **Unterverzeichnis** erstellt. Dort können alle Dokumente zu dieser jeweiligen Pflicht abgelegt werden.
2. **Dokumente aller Art** können im Unterverzeichnis „*_Allgemeines*“ gespeichert werden, sofern sie pflichtübergreifend relevant sind.
3. OPTIONAL :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

Dies soll im Folgenden erläutert werden:

1.10.1 Zu 1: Ein Unterverzeichnis für jede Pflicht

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

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



Hier können Sie ggf. auch die Dokumente zum PDCA-Zyklus speichern, so wie es bei den allgemeinen Bearbeitungshinweisen auf Seite 24 beschrieben ist. Auch die Formulare des Kapitels 12 (ab Seite 308) können hier gespeichert werden; die entsprechenden Dateinamen werden in den jeweiligen Unterkapiteln bereits vorgeschlagen.

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

Die Verzeichnisnamen tragen nicht nur das Kürzel, sondern zusätzlich auch die Überschrift der jeweiligen Pflicht. Im Oktober 2018 sind viele hilfreiche Unterverzeichnisse und „_liesmich.txt“-Dateien hinzugekommen. Außerdem wurden einige Formulare und Checklisten aus dem hier vorliegenden PrivazyPlan® in ein MS-Word-Dokument übernommen, um es leicht bearbeiten zu können.

1.10.2 Zu 2: Ein Unterverzeichnis für Dokumente aller Art

Sie werden allgemeine Dokumente im Rahmen des PrivazyPlan® speichern wollen. Dafür finden Sie Platz in dem Verzeichnis „*_Allgemeines*“.

Hier können Sie beispielsweise auch Fachliteratur speichern, wie beispielsweise das empfehlenswerte eBook „DS-GVO im Überblick“ in Deutsch und Englisch (siehe Seite 310). Der PrivazyPlan® liefert hier auch eine Mindmap-Grafik zu allen Pflichten (siehe Seite 696).

Weiter zur nächsten Station der Tour >

1.10.3 Zu 3: PrivazyPlan.xlsx

[Vorab ein wichtiger Hinweis: Bei den Verantwortlichen, die mittels DSB-MIT-SYSTEM® betreut werden, ist diese MS-Excel-Tabelle ohne Relevanz. Wir nutzen die Software DSB-Reporter®, um die Pflichterfüllung zu dokumentieren. Ein ausführlicher Fragenkatalog in dem Standard-Dokument DOC_071 („dsb_pflichtüberwachung.doc“) stellt die richtigen Fragen. Insofern spielt die hier vorgestellte PrivazyPlan.xls keine Rolle.]

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

a) Tabellenblatt „Pflichten der Verarbeitungen“

Hier kann für jede einzelne Verarbeitung die Prüfung der Pflichten vorgenommen werden.
Dies betrifft jene Pflichten in dem Mindmap in der PrivazyPlan.xls (siehe Seite 29), die über dem blauen Strich erscheinen.
Konkrete Beispiele für Verarbeitungen finden sich auf Seite 404.

b) Tabellenblatt „Pflichten des Unternehmens“

Hier können die allgemeinen Pflichten (also jene, die unabhängig von den speziellen Verarbeitungen sind) kurz dokumentiert werden.
Dies betrifft jene Pflichten in dem Mindmap in der PrivazyPlan.xls (siehe Seite 29), die unter dem blauen Strich erscheinen.

c) Tabellenblatt „BDSG_004“ etc.

Für jede Pflicht kann ein eigenes Tabellenblatt angelegt werden. Hier können alle Angaben des PDCA-Zyklus gespeichert werden. Dies ist also gewissermaßen eine super-minimale Form eines Datenschutz-Managementsystems.

Die Tabelle ist so konfiguriert, dass die Zeilenhöhe dynamisch an den Text angepasst wird. Mit ALT+ENTER können Sie Zeilenumbrüche einfügen.

- In der **Plan**-Zeile tragen Sie alle Ihre Planungs-Überlegungen ein.
- In der **Do**-Zeile dokumentieren Sie Ihre konkreten Handlungen. Neue Einträge fügen Sie optimalerweise oben in die Zeile ein. Nennen Sie auch das Datum und das Namenskürzel des Mitarbeiters.
- In der **Check**-Zeile dokumentieren Sie die konkreten Überprüfungen. Neue Einträge fügen Sie optimalerweise oben in die Zeile ein. Nennen Sie auch das Datum und das Namenskürzel des Mitarbeiters.
- In der **Act**-Zeile dokumentieren Sie die konkreten Handlungsempfehlungen. Neue Einträge fügen Sie optimalerweise oben in die Zeile ein. Nennen Sie auch das Datum und das Namenskürzel des Mitarbeiters.

d) Tabellenblatt „plan“

Hier werden einfach nur die „Plan“-Texte aller Pflichten tabellarisch zusammengeführt. Somit kann man auf einen Blick sehen, welche Planungen konkret vorgenommen wurden.

e) Tabellenblatt „check“

Hier werden einfach nur die „Check“-Texte aller Pflichten tabellarisch zusammengeführt. Somit kann man zweierlei erkennen: (a) Wann ist die nächste Prüfung fällig und (b) was wurde zuletzt geprüft.

Beachten Sie: In der letzten Spalte gibt es einen Hyperlink mit dem Text „Verzeichnis öffnen“. Hiermit können Sie das jeweilige Pflicht-Unterverzeichnis direkt öffnen.

1.10.4 Sonstige Überlegungen

- Wo sollen die Dateien abgelegt werden?
- Wer kopiert die aktuelle Datenstruktur auf Ihren lokalen PC? Wer löscht die anfänglichen Demo-Dateien heraus? Wer hat einen Blick darauf, ob sich die Vorlage (also XLS und Verzeichnisstruktur) ändert und dementsprechend auch in Ihrer lokalen Kopie geändert werden sollen?
- Wer soll lesenden Zugriff haben?
- Wer soll schreibenden Zugriff haben?
- Soll der Datenschutzbeauftragte hier seine Überwachungsfunktion wahrnehmen können?
- Soll eine regelmäßige Kopie der Verzeichnisstruktur erstellt werden, damit eine (einigermaßen) verbindliche Historie zu erkennen ist?
- Nach welchem Muster sollen die Dateinamen vergeben werden?
- Sollen die Dateien eher im MS-Word-Format abgelegt werden, oder eher im PDF-Format (in welchem die Inhalte nicht versehentlich geändert werden können)?

1.11 Die wichtigsten „Werkzeuge“ (zip, Transparenztext, Stammblatt, ...)

Einleitung

Sie planen Datenschutz-Compliance? Dafür bieten wir Ihnen einige sehr wertvolle „Werkzeuge“:

1.11.1 PrivazyPlan.zip

In einer umfangreichen ZIP-Datei stellen wir Ihnen wertvolles Knowhow zur Verfügung. Es geht hier um zwei Aspekte:

a) Formular-Vorlagen

Auch im Datenschutz gilt: Eine hohe Qualität lässt sich nur mit guten Checklisten und Anleitungen sicherstellen. Daher haben wir im Kapitel 12 auf den Seiten 310-464 ausführliche und praxisbewährte Formulare erarbeitet. Wir stellen diese Dokumente auch im DOCX-Format zur Verfügung, damit Sie die Formulare am Computer ausfüllen können. Siehe Seite 29.

Wir empfehlen Ihnen dringend diese (fast monatlich aktualisierte) Formular-Sammlung auf Ihren lokalen PC herunterzuladen und bei Bedarf anzuwenden!

Ohne diese Formulare sind Sie letztlich völlig hilflos, wenn beispielsweise eine betroffene Person ihre Persönlichkeitsrechte einfordert (siehe Kapitel 38). Alle Abteilungs- und Fachbereichsleiter sollten diese Formulare kennen und anwenden.

➔ Wir liefern Ihnen alle notwendigen Formulare stets aktuell im DOCX-Format.

b) Verzeichnisstruktur der Pflichten

Es gibt ca. 50 bußgeldbewehrte Pflichten, deren Einhaltung der Verantwortliche dokumentieren muss. Doch wie organisiert man diese Flut an Dokumenten? Wir schlagen in der PrivazyPlan.zip-Datei vor, dass Sie für jede Pflicht (-Erfüllung) ein eigenes Unterverzeichnis erstellen.

Auf den ersten Blick sind 50 Unterverzeichnisse ein „ganz schöner Wust“, aber sehr schnell werden Sie die Hemmung verlieren und sich daran erfreuen, dass alle Dokumente systematisch (und eng an den PrivazyPlan® angelehnt) dokumentiert sind.

Bedenken Sie die **personellen Wechsel**, die in einem Unternehmen unvermeidlich sind. Wenn jeder die Dokumente so speichert, wie er es gerade für richtig hält, dann ist nach kurzer Zeit das Chaos programmiert. Vertrauen Sie auf unsere Erfahrung.

Bedenken Sie die **positive Wirkung auf Auditoren und Aufsichtsbehörden**, wenn die Dokumente derart systematisch gespeichert werden. Das schafft Vertrauen!

Die gewünschten Dokumente werden schnell gefunden und somit sind Audits (intern oder extern) schnell erledigt. Auch Ihr Datenschutzbeauftragte wird Ihnen danken, denn er hat gemäß Artikel 39 (1b) eine Überwachungspflicht.

➔ Wir liefern Ihnen eine Verzeichnisstruktur, die über Jahre für Ordnung sorgt.

1.11.2 Transparenztexte

Station 5: Transparenz schaffen

Die von Artikel 13 geforderte Informationspflicht hat es in sich: Zum Zeitpunkt der Datenerhebung muss die betroffene Person umfassend informiert werden. Dies ist eine öffentlichkeitswirksame Pflicht und daher so wichtig.

Weil alle auskunftspflichtigen Informationen letztlich auf dem Verarbeitungsverzeichnis beruhen, ist jene (zeitaufwändige) Dokumentation letztlich die Grundlage für Transparenz.

Hier im PrivazyPlan® propagieren wir „Transparenztexte“, die auf der Website des Unternehmens veröffentlicht werden können.

< Zurück • Home • Weiter >

Eine wichtige Säule des Datenschutzes ist TRANSPARENZ. Dies wird schon allein daran ersichtlich, dass die Artikel 13, Artikel 14 und Artikel 15 sich intensiv um Transparenz bemühen.

Siehe Pflichten **[GVO_013]**, **[GVO_014]** und **[GVO_015]** auf Seite 40, 50, 55.

Hier im PrivazyPlan® werden diese Pflichten sehr ernst genommen und im Konzept der „Transparenztexte“ sehr effizient erfüllt. Für jede einzelne Datenverarbeitung soll ein eigener Transparenztext erstellt werden.

Aus diesem Grund besteht die „weiche“ Pflicht [AUX_011] im Sinne einer „Strategie“ zur effizienten Informations- bzw. Auskunftserteilung in Form von Transparenztexten (siehe Seite 324).

a) WARUM ist Transparenz wichtig?

Der offensichtlichste Grund ist die Gefahr von Geldbußen.

Wer die betroffenen Personen nicht frühestmöglich (und vollständig) informiert, der riskiert ein Bußgeld gemäß Artikel 83 (5b) von bis zu 4% vom weltweiten Jahresumsatzes. Reine Theorie? Nun, gegen google wurde deswegen in Frankreich eine Geldbuße von 50 Mio. € verhängt (siehe Seite 579). Überzeugt?

Wer die Auskunftspflicht gemäß Artikel 15 nicht rechtzeitig und vollständig erfüllt, dem droht das gleiche Bußgeld. Das ist besonders kritisch, denn häufig sind es unzufriedene Kunden und Mitarbeiter, die derlei Auskünfte einfordern. Sie hoffen, dass das Ergebnis unvollständig ist, um dann Ärger machen zu können (meist wird mit einer Beschwerde bei der Aufsichtsbehörde gedroht).
[Nebenbei bemerkt: Es bleibt in diesem Zusammenhang immer noch die leidige Frage hinsichtlich des Rechts auf „Datenkopie“ gemäß der Pflicht [GVO_015a] auf Seite 58].

Aus diesen Gründen schlagen wir vor: Sammeln Sie alle Informations- und Auskunftsaspekte einer Verarbeitung und publizieren Sie diese sofort im Internet (bzw. Intranet). Dann kann sich jede betroffene Person über alle erdenklichen Aspekte informieren. Feindlich gesinnten Personen ist der Wind größtenteils aus den Segeln genommen.

Ergebnis: **(a)** Die betroffenen Personen sind zufrieden und „nerven“ nicht mit Auskunftsforderungen, **(b)** die Aufsichtsbehörde sieht, dass Sie sich kümmern, **(c)** Sie sparen viel Zeit und Nerven und können sich um Ihr Kerngeschäft kümmern.

Aus unserer Sicht gibt es keine sinnvolle Alternative zu den Transparenztexten. Machen Sie sich selbst ein Bild unter www.SecureDataService.de/transparenz.

b) WIESO in Form von Transparenztexten?

Es gibt bestimmt viele Wege, um für Transparenz zu sorgen. Warum vertreten wir den Weg der „Transparenztexte“? Wenn man die Artikel 13-15 liest, dann wird schnell klar, dass die ca. 20 Aspekte der Informations- und Auskunftspflichten zu einer Datenverarbeitung in jeweils einem gemeinsamen Text erfüllt werden sollten.

Sie könnten natürlich auch die Angaben der Artikel 13-15 in drei verschiedenen Texten niederschreiben. Doch das macht viel mehr Arbeit. Und es besteht die Gefahr, dass die Inhalte voneinander abweichen. Das macht einfach keinen Sinn.

Was sagen die **Aufsichtsbehörden** dazu?

- Die Artikel-29-Datenschutzgruppe (siehe Seite 599) hat im Workingpaper „WP 260“ im April 2018 sehr ausführlich Stellung genommen zu allen Fragen der Auskunftspflicht bezüglich Artikel 13 und Artikel 14. Siehe Seite 42. Dort wird genau das gefordert, was wir mit den Transparenztexten erfüllen.

- Die NRW-Aufsichtsbehörde hat am 11.01.2019 eine sehr ausführliche Umsetzungshilfe zu den Datenschutzhinweisen publiziert. Dort werden genau jene Punkte genannt, die auch unsere Transparenztexte aufweisen.

- Die Bayerische Aufsichtsbehörde warnt, dass oberflächliche Informationstexte nicht ausreichen:
  *" Es muss dabei jedoch sichergestellt werden, dass nicht auf **eine** allgemeine "Datenschutzinformation für alle Fälle" verwiesen wird, sondern, dass der interessierte Betroffene insbesondere erkennt, was die Rechtsgrundlage der Verarbeitung in seinem speziellen Fall ist. Es kann daher im Zweifel **keine** **"One-Size-Fits-All-Information"** für alle betroffenen Personen also Beschäftigte, Kunden, Geschäftspartner, Webseitenbesucher und Lieferanten geben.“*
  Die Datenschutz-PRAXIS 02/2019 erläutert diesen Ansatz auf Seite 15-17. Es wird genau das beschrieben, was die Transparenztexte liefern.

Spätestens jetzt sollte klar sein, dass die Transparenztexte sinnvoll sind und letztlich von den Aufsichtsbehörden genau so empfohlen werden. Schauen Sie sich das Beispiel unter www.SecureDataService.de/transparenz an, und Sie werden verstehen, wie mächtig dieses Werkzeug ist.

c) WANN müssen die Transparenztexte bereitgestellt werden?

Die betroffenen Personen sollen Artikel 13 **zum Zeitpunkt der Erhebung der Daten** informiert werden. Es reicht eben nicht aus, diese Informationen und Auskünfte „auf Antrag“ zur Verfügung zu stellen.

Mit anderen Worten: Wo auch immer Daten bei betroffenen Personen abgefragt werden, dort müssen Sie zuallererst die Informationspflichten erfüllen. Das ist vergleichbar zur Datenschutzerklärung einer Website: Erst informieren, dann nutzen. Das gilt übrigens auch für Papier-Formulare!

Aus diesem Grund empfehlen wir die „vorbeugende“ Publikation dieser Texte. Jede betroffene Person kann sich jederzeit ein Bild von der Datenverarbeitung machen.

Sie müssen dann einfach nur noch an den passenden Stellen auf den jeweiligen Transparenztext verweisen. Beispielhaft sehen Sie dies auf www.SecureDataService.de/cisco-webex-meetings.htm.

d) WAS beinhalten die Transparenztexte?

Der Startpunkt ist das Verarbeitungsverzeichnis gemäß Artikel 30 (siehe Pflicht **[GVO_030]** auf Seite 110).
Dort sind alle Verarbeitungen aufgelistet und bereits mit Name, Zweck, Empfängern, Löschfrist, Daten, Betroffenen und Drittland-Garantien (von Übermittlungen und Auftragsverarbeitungen) dokumentiert.

Hinzu kommt die Angabe gemäß Artikel 15 die Persönlichkeitsrechte, das Beschwerderecht, ggf. Aspekte zur automatisierten Entscheidung bzw. Profiling.

Hinzu kommt die Angabe gemäß Artikel 14 die Kontaktdaten des Datenschutzbeauftragten, die Rechtsgrundlage, die ggf. berechtigten Interessen des Verantwortlichen, ggf. das Widerrufsrecht von Einwilligungen.

Hinzu kommen die Angaben gemäß Artikel 13 ggf. die vertraglichen Notwendigkeiten und die Folgen der Nicht-Bereitstellung.

Hinzu kommt gemäß Artikel 26 ggf. eine Liste von Angaben zur gemeinsamen Verantwortlichkeit mit anderen Unternehmen. Spätestens seit den Facebook-Fanpages ist dies ein heikles Thema.

… das war’s. Diese Angaben stellen Sie einmal zusammen und dann haben Sie Ruhe. Für jede Datenverarbeitung haben Sie dann einen individuelle Transparenztext zur Hand.

[Wird Ihr Unternehmen durch einen Datenschutzbeauftragten betreut, der im Rahmen von DSB-MIT-SYSTEM® tätig ist? Dann kann er Ihnen die Transparenztexte automatisiert aus dem Verarbeitungsverzeichnis heraus erstellen. [9] So gesehen sind die Transparenztexte ein „Nebenprodukt“ des ausführlichen Verarbeitungsverzeichnisses. Das kostet Sie als Kunde keine Minute Ihrer Zeit.]

e) WO werden die Transparenztexte publiziert?

Publizieren Sie die Transparenztexte der „öffentlichkeitswirksamen“ Verarbeitungen (z.B. bezüglich Kunden, Interessenten und Lieferanten) auf der **Website**
Publizieren Sie die firmeninternen Verarbeitungen (z.B. bezüglich der eigenen Beschäftigten) im **Intranet**.

Diese beiden Orte kann sich jeder Mitarbeiter merken und somit den betroffenen Personen jederzeit schnell Auskünfte geben. Jeder weiß Bescheid. Besser geht’s nicht, oder?

Wo auch immer Sie personenbezogene Daten erheben: Verweisen Sie direkt auf den jeweiligen Transparenztext. Auf Websites können Sie einen Hyperlink setzen. Auf Papierformularen können Sie die URL abdrucken und/oder mittels QR-Code auf die URL verlinken.

www.SecureDataService.de/Transparenz

Probieren Sie es aus, indem Sie diesen QR-Code mit Ihrem Smartphone fotografieren. In manchen Betriebssystemen wird die dahinterliegende URL sofort erkannt. Andernfalls müssen Sie eine QR-Code-Reader-App installieren.

Unser Dank an
www.qrcode-monkey.com
mit großartigen Gestaltungsmöglichkeiten!

Die c’t 20/2021 empfiehlt auf Seite 85 den Offline-QR-Generator unter www.nir.net der offline funktioniert.

[9] Die Software DSB-Reporter® bietet die „Export“-Funktion, um alle Transparenztexte zu erzeugen. Zuvor wurde in jeder einzelnen Verarbeitung das „Ziel“ des Transparenztexte spezifiziert (intern/öffentlich/Betriebsrat/ …). Für das betreute Unternehmen werden dann einmalig die Dokumentvorlagen gestaltet (mit Logo und Impressums-Link etc.). Dann wird der Export gestartet. Die Ergebnisdateien liegen dann auch gezippt vor, um sie dem betreuten Unternehmen bequem per E-Mail liefern zu können.

Dieser simple und logische Ansatz wird bei Mitarbeitern und Kunden mit Sicherheit auf Zustimmung stoßen und Vertrauen schaffen.

Wo kann das verantwortliche Unternehmen die Transparenztexte lokal speichern und dauerhaft dokumentieren? Wir schlagen vor:

\PrivazyPlan\AUX_011
… dort können Sie Ihre Transparenztexte speichern. (Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

[Wird Ihr Unternehmen durch einen Datenschutzbeauftragten betreut, der im Rahmen von DSB-MIT-SYSTEM® tätig ist? Dann erhalten Sie die Transparenztexte in Form von HTML-Dateien mitsamt Inhaltsverzeichnis. Sie können diese Dateien dann per Copy&Paste auf den Webserver kopieren. Das kostet Sie als Kunden maximal fünf Minuten Ihrer Zeit.]

f) … und langfristig?

Die Transparenztexte müssen selbstverständlich stets aktuell gehalten werden.

Wenn also Datenverarbeitungen hinzukommen oder beendet werden, dann ändert sich die Liste der Transparenztexte. Und wenn sich Details ändern (z.B. Datenkategorien oder betroffene Personen), dann müssen die betroffenen Transparenztexte aktualisiert werden.

Letztlich müssen also die Veränderungen am Verarbeitungsverzeichnis beobachtet werden und ggf. zu neuen Transparenztexten führen. Siehe Pflicht **[GVO_030]** auf Seite 110.

[Wird Ihr Unternehmen durch einen Datenschutzbeauftragten betreut, der im Rahmen von DSB-MIT-SYSTEM® tätig ist? Dann werden die Änderungen am ausführlichen Verarbeitungsverzeichnis spätestens am Folgetag automatisiert an den Datenschutzbeauftragten gemeldet [10] und er wird Ihnen die aktuellen Transparenztexte zur Verfügung stellen.]

[10] Die Software DSB-Reporter® erzeugt die sogenannten „Verarbeitungs-Logfiles“, wo alle wichtigen Änderungen an einer Verarbeitung dokumentiert werden. Diese Dateien werden dem Datenschutzbeauftragten per E-Mail zugeleitet, der dann sofort handelt, indem er die Transparenztexte erneut exportiert und dem betreuten Unternehmen zur Verfügung stellt. [Der Dokumentationsstatus der jeweiligen Verarbeitung muss mindestens „Bereit für Transparenztext“ lauten.] Insofern ist automatisiert sichergestellt, dass relevante Änderungen am Verarbeitungsverzeichnis zu „frischen“ Transparenztexten führen.
… es bleibt also nur noch die Herausforderung, dass z.B. eine veränderte Löschfrist dem Datenschutzbeauftragten unverzüglich mitgeteilt wird… aber das ist ein anderes Thema… 😉]

g) Fazit zu den Transparenztexten

Aus unserer Sicht sind die Transparenztexte alternativlos. Nur mit deren Hilfe können Sie rechtzeitig und vollständig informieren bzw. ausführlich beauskunften (von dem Recht auf „Datenkopie“ einmal abgesehen).

Aus diesem Grund besteht die „weiche“ Pflicht **[AUX_011]** im Sinne einer „Strategie“ zur effizienten Informations- bzw. Auskunftserteilung in Form von Transparenztexten (siehe Seite 324).

➔ Wir liefern Ihnen mit dem Konzept der „Transparenztexte“ ein extrem effizientes Werkzeug, um die grundlegenden Informations- und Auskunftspflichten zu erfüllen. Im Rahmen von DSB-MIT-SYSTEM® erhalten Sie diese Texte in Form von HTML-Dateien, die Sie in kürzester Zeit publizieren können.
Das ist die perfekte Kombination von Rechtssicherheit und Effizienz!

1.11.3 Stammblätter

Der PrivazyPlan® „funktioniert“ – wie auf Seite 12 beschrieben - folgendermaßen: Die DS-GVO erlegt den Verantwortlichen **ca. 50 Pflichten** auf, die sich allesamt im Bußgeldkatalog des Artikel 83 finden. Diese Pflichten werden hier im PrivazyPlan® ausführlich beschrieben und mit Checklisten und Vorlagen handhabbar gemacht (siehe Seite 12).

Wenn jede einzelne Pflicht bearbeitet wurde… und erst dann!... kann das Unternehmen von sich behaupten alle bußgeldbewehrten Pflichten unter Kontrolle zu haben. Nur dann ist dafür auch ein Nachweis erbringbar.

Würde man auch nur eine einzige Pflicht ignorieren oder übersehen, so könnte es passieren, dass die Aufsichtsbehörde genau hier ein Bußgeld verhängt, weil sich eine betroffene Person genau über diese eine Pflicht echauffiert und beschwert hat. Keine Pflicht ist wichtiger als eine andere, denn überall drohen Bußgelder von bis zu 10-20 Mio. Euro (bzw. Schadenersatzforderungen… siehe Seite 582).

⚠ Das hier vorgeschlagenen Stammblätter einer jeden (Daten-) Verarbeitung ist der Dreh- und Angelpunkt zur Erfüllung vieler Datenschutzpflichten. Das Bearbeiten der Stammblätter ist unvermeidlich, um wirklich alle bußgeldbewehrten Pflichten systematisch zu erfüllen.

a) WARUM gibt es Stammblätter?

Das Konzept der „Stammblätter“ ist eine Innovation im Rahmen des PrivazyPlan®. Unseres Wissens nach arbeiten andere Datenschützer nicht derart systematisch [11]. Für jede (Daten-) Verarbeitung wird ein eigenes „Stammblatt“ erzeugt und ausgefüllt.

Wir haben uns für die **Bezeichnung „Stammblatt“** entschieden, weil dieses Dokument alle grundlegenden Informationen beinhaltet und zukünftigen Änderungen berücksichtigt. Es begleitet die (Daten-) Verarbeitung über den gesamten Zeitraum, in dem sie ausgeführt wird.

Im Kern geht es darum: Ca. 15 Datenschutz-Pflichten muss man konkret für jede einzelne (Daten-) Verarbeitung erfüllen: z.B. für Personalakte, Website, Videoüberwachung, Marketingmaßnahmen, Betriebsrats-Tätigkeiten etc.

Im Folgenden erfahren Sie alles Wichtige über die Stammblätter…

b) WIE werden die Stammblätter erzeugt?

Prinzipiell finden Sie ein Blanko-Formular auf Seite 411. Verlieren Sie nicht den Mut, auch wenn Ihnen jene Blanko-Vorlage erschlagend lang erscheint. Denn nicht jeder Aspekt spielt bei jeder (Daten-) Verarbeitung eine Rolle (siehe das folgende Kapitel).

[Wird Ihr Unternehmen durch einen Datenschutzbeauftragten betreut, der im Rahmen von DSB-MIT-SYSTEM® tätig ist? Dann werden Stammblätter vom Datenschutzbeauftragten automatisiert erzeugt. [12] Als Kunde müssen Sie dann nur noch die ca. 15 offenen Punkte ausfüllen. Das spart erheblich Zeit und Nerven. Der Newsletter NEWS_041 („news_stammblatt“) erklärt dies den Mitarbeitern.]

c) WAS beinhalten die Stammblätter?

Die gute Botschaft lautet: Von den ca. 50 bußgeldbewehrten Pflichten müssen letztlich für jede (Daten-) Verarbeitung nur ca. 15 Aspekte bearbeitet werden. In diesem Zusammenhang ist das Mindmap auf Seite 696 Interessant: Dort sind alle Pflichten aufgeführt und eine blaue Linie trennt die „allgemeinen“ Pflichten von den verarbeitungs-spezifischen Pflichten.

Dies wird im Folgenden genau erklärt:

- **Nicht enthalten sind ca. 20 Pflichten, die unternehmensübergreifend bearbeitet** werden. Der Verantwortliche kümmert sich einmal um diese Fragestellung… und die jeweilige Aufgabe ist erfüllt. Diese Pflichten werden im automatisiert erstellten Stammblatt NICHT aufgeführt. Dies sind insbesondere:

  - Nachweis der Einhaltung der Grundsätze **[GVO_005]**
  - Verarbeitungsverzeichnis erstellen **[GVO_030]** etc.
  - Informations-Sicherheits-Managementsystem einrichten **[GVO_032]**
  - Umgang mit Datenschutzverletzungen **[GVO_033]** etc.
  - Datenschutzbeauftragten benennen **[GVO_037]** etc.
  - Berufliche Schweigepflicht **[STGB_203]**
  - Unzumutbare Werbebelästigung vermeiden **[UWG_007]**

- **Nicht zu beantworten sind ca. 15 Pflichten** die zwar prinzipiell für jede einzelne (Daten-) Verarbeitung relevant sind, die im Rahmen des Verarbeitungsverzeichnisses **bereits beantwortet** wurden, oder wo sich die eine Pflicht im Einzelfall **irrelevant** herausstellt (z.B. Einwilligungs-Dokumentation mangels „Einwilligung“ als Rechtsgrundlage). Diese Pflichten werden im automatisiert erzeugten Stammblatt bereits „beantwortet“ und bedürfen allenfalls der Kontrolle. Dies sind insbesondere:

  - Rechtmäßigkeit der (Daten-) Verarbeitung **[GVO_006]**
  - Bei Erhebung von Daten ausführlich informieren **[GVO_013]**
    (Geschieht durch die Transparenztexte.)

[11] Woran erkennt man, ob ein Datenschützer systematisch alle Bußgeldrisiken berücksichtigt? Ganz einfach: Fragen Sie ihn „*wie viele bußgeldbewehrte Pflichten birgt die DS-GVO in sich?*“. Falls er zögert oder die Frage nicht einmal versteht, dann wird er Ihnen keine systematische Betreuung bieten können; es ist dann „Glücksache“, ob er wirklich alle Risiken erkannt hat und Sie dementsprechend betreut.

[12] Die Software DSB-Reporter® bietet eine Export-Funktion, mit der Stammblätter erzeugt werden können. Zuvor müssen **(a)** die Verarbeitungen dort vollständig dokumentiert sein und **(b)** die Transparenztexte müssen fehlerfrei und aussagekräftig sein. Die HTML-Dokumente mit dem Dateityp *.doc werden dann einmalig (!) dem Kunden ausgehändigt.

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 (siehe Seite 582).

Die Aspekte der Persönlichkeitsrechte werden auch in der VdS-Richtlinie 10010 (Seite 512) im dortigen Kapitel 10.12 („Betroffenenrechte“) thematisiert.

➔ Die allgemeinen Erwägungen zur Gewährleistung der Persönlichkeitsrechte sind in der Checkliste „**Allgemeine Bearbeitungshinweise (zum PDCA-Zyklus)**“ zusammengefasst (siehe Seite 24). Jenes Kapitel ist von entscheidender Wichtigkeit!

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

2.0.1 Fristen zur Wahrung der Persönlichkeitsrechte

Für sämtliche Pflichten des Kapitel III der DS-GVO („Rechte der betroffenen Personen“) unterliegen den Fristen, die im Artikel 12 (3) genannt werden.

Davon betroffen sind die Artikel 15-22; also alle Pflichten, die hier im Kapitel 2 („Pflichten aufgrund von Persönlichkeitsrechten“) auf den Seiten 38-98 beschrieben sind.

Demnach sollte man die Persönlichkeitsrechte **unverzüglich** (also ohne schuldhaftes Verzögern) sicherstellen. Die DS-GVO nennt hier einen Zeitraum von **einem Monat** nach Beantragung durch die betroffene Person. Im Einzelfall ist eine verlängerte Frist möglich.

2.0.2 Missbräuchliche Nutzung der Persönlichkeitsrechte?

Bei offenkundig **unbegründeten oder „exzessiven“ Anträgen** gemäß der Persönlichkeitsrechte aus Artikel 15 bis 21 liefert der Artikel 12 (5) die Möglichkeit, dass sich der Verantwortliche weigert (oder ein angemessenes Entgelt fordert). Die DS-GVO präzisiert dies in keiner Form und auch die Fachwelt äußert sich nicht zu diesem Aspekt.
Die britische Aufsichtsbehörde hat im Juli 2021 dazu eine Orientierungshilfe geliefert (siehe auch hier). Die deutschen (Arbeits-) Gerichte haben aber bis zum Juli 2021 nicht erkennen lassen, dass es hier irgendwelche Grenzen gäbe. Insofern ist es ziemlich riskant z.B. die Auskunfts- und Datenkopie-Verlangen abzulehnen. Auch die deutschen Aufsichtsbehörden werden an diesem Punkt wohl nur sehr wenig Verständnis zeigen.

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. [13]

Dieser Pflicht wird das Kürzel **[GVO_013]** zugeordnet (siehe Seite 14).

2.1.1 Allgemeine Informationen zur Pflicht [GVO_013]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● 40-seitige Orientierungshilfe aus Bayern ● Ausführliche Hinweise in der ULD-Praxisreihe 4 auf 18 Seiten. ● Die Aufsichtsbehörde in Brandenburg bietet ein Informationsblatt ● DSK-Kurzpapier-10 ● Die 11-seitige GDD-Praxishilfe DS-GVO VII („Transparenzpflichten“), auch in Englisch . ● Trainingseinheit 6 („Betroffenenrechte und Informationspflichten“) der Informationsreihe „Fit für die Datenschutz-Grundverordnung“.

2.1.2 Was bedeutet diese Pflicht [GVO_013] ?

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

Für den Begriff „**Erhebung** von Daten“ (engl. „collect“) liefert die DS-GVO im Artikel 4 leider keine Definition. In Deutschland lieferte der § 3 Abs. 3 BDSG-alt diese Definition: „*Erheben ist das **Beschaffen** von Daten über den Betroffenen*“. Es ist wohl davon auszugehen, dass hier eine AKTIVITÄT des Verantwortlichen vorliegen muss (siehe hier und hier und hier in RdNr. 15-16) . [14] Dementsprechend fallen unverlangt zugesendete Daten vermutlich nicht unter diese Informationspflicht.

Leider ist die Sachlage nicht besonders klar. Es besteht stets die Gefahr, dass eine betroffene Person (oder ein Wettbewerber) hier eine unterlassene Information wittert und sich beschwert bzw. eine Abmahnung ausspricht (siehe Seite 590).

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

1. Der Verantwortliche stellt auf einer Messe eine **Visitenkarten-Sammelbox** auf, wo die Messebesucher Ihre Visitenkarten einwerfen können. Es ist geplant, dass diese Daten in einer Customer-Relation-Management-Software (CRM) gespeichert werden. Es handelt sich hier also ganz klar um eine zielgerichtete Datenerhebung. Die betroffenen Personen müssen also informiert werden.
2. Der Verantwortliche **erhält beiläufig die Visitenkarten** von Gesprächspartnern im Rahmen von Messe-Gesprächen. Das Ziel ist eine mehr oder weniger diffuse Kontaktaufnahme, um über Geschäftsanbahnung zu sprechen. Dies ist keine gezielte und zielgerichtete Erhebung und bedarf keiner Information. Siehe auch die entsprechende FAQ-11 der Bayerischen Datenschutz-Aufsichtsbehörde.

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

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

2. Auf der normalen Geschäftsnummer **nennt eine Person ungefragt Daten**. Zum Zeitpunkt des Gesprächs lässt sich noch gar nicht vollständig bestimmen, ob und wo die Daten gespeichert werden. Erwartet die DS-GVO, dass wir jeden Anrufer über mögliche (digitale) Gesprächsnotizen informieren müssen? Das ist wohl eher nicht zumutbar.

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

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

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.2 Zweckänderung vorab mitteilen [GVO_013a]

Persönlichkeitsrechte

Gemäß Artikel 13 (3) bzw. Artikel 14 (4) muss die betroffene Person über geplante Zweckänderungen vorab informiert werden. Möglicherweise hat die betroffene Person ein Widerspruchsrecht, falls sie glaubt, dass ihre „Rechte und Freiheiten“ unzulässig beschnitten werden. Die DS-GVO nennt diesen Vorgang auch „*Weiterverarbeitung*“ (engl. „*further processing*“).

Diese Pflicht ist insofern speziell, als dass sie **zwei** verschiedene Artikel mit gleichlautenden Verpflichtungen betrifft. Durch diese Zusammenfassung wird der PrivazyPlan® nicht unnötig aufgebläht.

Dieser Pflicht wird das Kürzel **[GVO_013a]** zugeordnet (siehe Seite 14).

2.2.1 Allgemeine Informationen zur Pflicht [GVO_013a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Siehe auch die Pflicht **[GVO_006a]** zu sorgsamen Prüfung von Zweckänderungen auf Seite 137.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Beispielsweise die 11-seitige GDD-Praxishilfe DS-GVO VII („Transparenzpflichten“).

[Im Rahmen des PrivazyPlan® wird das Dossier „Zweckbindung“ und das Dossier „Zweckänderung“ 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.]

2.2.2 Was bedeutet diese Pflicht [GVO_013a] ?

a) Wann muss informiert werden?

Eine Informationspflicht in Richtung der betroffenen Personen kann bestehen, wenn nach sorgsamer Prüfung eine Zweckänderung (im Sinne von „Weiterverarbeitung“) geplant ist. Dies muss gemäß Artikel 6 (4) vorab sorgsam geprüft werden (siehe Pflicht **[GVO_006a]** auf Seite 137).
Diese Pflicht ist beispielsweise dann relevant, wenn personenbezogene Daten an die Polizei oder andere öffentliche Stellen übermittelt werden sollen (siehe Seite 535), denn in aller Regel ist dieser Verarbeitungszweck nicht vorab geplant.

Wenn sich die geplante Zweckänderung als zulässig herausstellt, dann müssen die betroffenen Personen gemäß Artikel 13 (3) bzw. Artikel 14 (4) vorab darüber informiert werden.

Die DS-GVO lässt sämtliche Details im Dunkeln: Wie früh muss informiert werden? Muss jede Person individuell informiert werden, oder reicht ein Aushang oder Hinweis in einem Webportal? Muss man nachweisen können, dass alle betroffenen Personen den Hinweis gelesen haben? Sollte man sich sicherheitshalber vielleicht sogar eine Lese-Bestätigung geben lassen? Kann ein Betriebsrat diese Information quasi „stellvertretend“ für die Belegschaft zur Kenntnis nehmen?

Es gibt zahlreiche Ausnahmen von dieser Informationspflicht (siehe folgendes Unterkapitel). Wenn keine dieser Ausnahmen greift, dann muss die Informationspflicht durchgeführt werden.

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite 39).

b) Wann muss NICHT informiert werden?

Es gibt zahlreiche Szenarien, wo eine Informationspflicht NICHT besteht.

1.) Die Daten wurden bei der Person selbst erhoben und die Person verfügt bereits über die notwendigen Informationen? Dann entfällt die Informationspflicht gemäß Artikel 13 (4).
(Dies könnte z.B. zutreffen, wenn die betroffene Person eine Einwilligung zu dieser Zweckänderung gegeben hat, und über die Auswirkungen ausführlich aufgeklärt wurde.)

2.) Die Daten wurden bei einem Dritten erhoben und die Person verfügt bereits über die notwendigen Informationen? Dann entfällt die Informationspflicht gemäß Artikel 14 (5a).

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.3 Bei Erhebung von Daten über Dritte informieren [GVO_014]

Persönlichkeitsrechte

Gemäß Artikel 14 (1) und Artikel 14 (2) muss der Verantwortliche die betroffenen Personen darüber informieren, dass ihre Daten an anderer Stelle (also durch einen Dritten) erhoben wurden. Dies geschieht spätestens innerhalb von vier Wochen. Doch es gibt auch zahlreiche Ausnahmen.

Dieser Pflicht wird das Kürzel **[GVO_014]** zugeordnet (siehe Seite 14).

2.3.1 Allgemeine Informationen zur Pflicht [GVO_014]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 33 Abs. 1 Nr. 2 BDSG **keine** Informationspflicht in Bezug auf die Absätze 1,2,4 und im Falle einer nicht-öffentlichen Stelle, falls **(a)** zivilrechtliche Ansprüche gefährdet wären oder **(b)** das Bekanntwerden die öffentliche Sicherheit gefährden würde. Doch muss der Verantwortliche dann gemäß § 33 Abs. 2 BDSG geeignete Maßnahmen treffen, um die berechtigten Interessen der betroffenen Personen zu schützen.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● 40-seitige Orientierungshilfe aus Bayern ● DSK-Kurzpapier-10 ● die 11-seitige GDD-Praxishilfe DS-GVO VII („Transparenzpflichten“).

2.3.2 Was bedeutet diese Pflicht [GVO_014] ?

Leider enthält die deutsche Übersetzung des Artikel 14 (1) einen kleinen **Fehler**: Es sollte heißen „*Wurden personenbezogene Daten nicht bei der betroffenen Person erhoben…*“ statt „*Werden…*“; der Grund dafür ist der englische Originaltext „*Where personal data have not been obtained from the data subject…*“. Auf der Seite www.privacy-regulation.eu wurde dies behoben.

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 davon aus, dass dies **nicht** so stimmt. In den folgenden Ausführungen wird angenommen, dass es allein um die Datenerhebung durch Dritte geht.

a) Was ist eine Erhebung durch Dritte?

Im normalen Geschäftsalltag eines typischen Unternehmens tritt diese Situation eher selten auf. Im Prinzip geht es darum, dass ein Verantwortlicher personenbezogene Daten über eine Person erhält, ohne diese Daten selbst erhoben (erfragt) zu haben.

Ein typisches Beispiel dafür ist der Fall eines Haftpflichtschadens: Die geschädigte Person meldet den Schaden der Versicherung und nennt natürlich auch den Namen des Verursachers. In diesem Fall erhält die Versicherung diese Daten des Verursachers durch einen Dritten. Die Versicherung muss dann gemäß Artikel 14 die betroffene Person (der Verursacher) über die Datenspeicherung und -Nutzung bei der Versicherung informieren.

Ähnliche Fälle liegen möglicherweise insbesondere vor bei

- Empfehlungswerbung (Kunden empfehlen Kunden)
- Whistleblower-Systemen (anonyme Meldung von Fehlverhalten einer beschäftigten Person, siehe Seite 430)
- Knöllchen z.B. nach zu schnellem Fahren mit dem Firmen-KFZ
- Meldung über neue Kunden von externen Vertriebspartnern
- Sämtliche Formulare, in welchen die Namen von anderen Personen genannt werden (so auch in Personalfragebögen, wo ggf. die Ehepartner genannt werden, um die Steuerklasse zu bestimmen)
- Ermittlungen durch Privatdetektive
- Öffentlich zugänglichen Quellen (z.B. Internet, Telefonbuch, Social Media)
- Ein anderes Beispiel für diese Dritt-Erhebung liefert die Pflicht **[GVO_008]** auf Seite 155: Dort kann ein Kind die E-Mail-Adresse eines Elternteils nen-

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.4 Auskunft erteilen [GVO_015]

Persönlichkeitsrechte

Das Recht auf Auskunft gemäß Artikel 15 (1) und Artikel 15 (2) ist sehr weitreichend. Die betroffenen Personen (bzw. Bevollmächtigte, wie z.B. Erben) müssen einen entsprechenden Antrag stellen. Es müssen **keine Details** beauskunftet werden. Diese Pflicht ist ernst zu nehmen, weil fehlende oder grob unvollständige Auskünfte von Jedermann leicht festzustellen sind.

Dieser Pflicht wird das Kürzel **[GVO_015]** zugeordnet (siehe Seite 14).

2.4.1 Allgemeine Informationen zur Pflicht [GVO_015]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) existieren zahlreiche Ausnahmen von der Auskunft-Pflicht (sofern sie nicht als unionsrechtswidrig anzusehen sind; siehe weiter unten).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: Lesenswert ist u.a. ● ZD 06/2019 Seite 239-245 (sehr theoretisch und ohne jedes konkrete Beispiel) ● das DSK-Kurzpapier-6 der Datenschutzkonferenz.

2.4.2 Was bedeutet die Pflicht [GVO_015] ?

Im Vergleich zum § 34 BDSG-alt müssen sehr viel mehr Details beauskunftet werden. Doch auch hier im Artikel 15 (1,2) gilt: Es müssen noch **keine Datendetails** geliefert werden; die Verordnung verlangt hier zunächst einmal nur die allgemeinen Daten-Kategorien (wie „Kontaktdaten“, „Bestelldaten“, „Nutzungsdaten“ etc.). Allerdings hat die betroffene Person gemäß Artikel 15 (3,4) das Recht auf eine Datenkopie (siehe folgendes Kapitel).

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite 39).

Bezüglich der **Dritterhebung** werden im Artikel 15 (1g) „alle verfügbaren Informationen über die Herkunft der Daten“ gefordert. Auf den ersten Blick ist anzunehmen, dass die genaue Firmierung des „Dritten“ genannt werden sollte.
Die Beschlüsse des Amtsgerichts Wertheim (Az. 1 C 66/19)) und des LG Mosbach (Az. 5 T 4/20) legen aber nahe, dass dies auch weitgehender interpretiert werden kann: WELCHE Daten wurden WANN von WEM erhoben? Siehe auch hier, hier und hier. Und dies schon in der allgemeinen Auskunfts-Phase
Eine Abgrenzung zur Datenkopie gemäß Artikel 15 (3) findet leider nicht statt (siehe Pflicht **[GVO_015a]** auf Seite 58).

Auch hinsichtlich **Drittland-Datentransfers** an Auftragsverarbeiter und (andere) Verantwortliche müssen beauskunftet werden. Der Erwägungsgrund 101 zum Artikel 44 betont, dass das europäische Datenschutzniveau nicht untergraben werden darf. Es gelten die Anforderungen der Artikel 44-50 (siehe Seite 210).

Der Verantwortliche darf einem Auskunfts-Ersuchen nicht durch **zu hohen Hürden erschweren**; die Niederländische Aufsichtsbehörde hat diesbezüglich ein Bußgeld von 830.000 € verhängt (*„Ab Mai 2018 beantragte das BKR eine Gebühr für den digitalen Abruf von Personendaten. Außerdem konnten die Menschen nur einmal im Jahr (per Post) kostenlos auf ihre Daten zugreifen. Dies ist nach der Datenschutzgesetzgebung nicht erlaubt. Daher wurde eine Geldbuße von 830.000 Euro verhängt*“; im Juli 2020 noch nicht rechtskräftig).

a) Eingeschränkte Auskunftspflicht in Deutschland

In Deutschland gibt es gemäß § 34 Abs. 1 Nr. 2 BDSG eine Ausnahme zur Auskunftspflicht. Demnach darf ein Verantwortlicher der betroffenen Person unter ganz bestimmten Bedingungen die Auskunft verweigern.

Die Gesetzesbegründung nimmt hier insbesondere Bezug auf den § 33 Abs. 2 Nr. 2 BDSG-alt („Benachrichtigung des Betroffenen“). Dort machte die vorliegende Regelung auch ganz offensichtlich Sinn. Doch die hier vorgenommene Übertragung auf das Auskunftsrecht wirkt manchmal befremdlich.

Die Details hierzu befinden sich in der Checkliste auf Seite 356. Es stellt sich heraus, dass die Regelung komplex ist und einen hohen bürokratischen Auf-

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.5 Datenkopie aushändigen [GVO_015a]

Persönlichkeitsrechte

Das Recht auf Datenkopien gemäß Artikel 15 (3) und Artikel 15 (4) gibt den Betroffenen ein (fast) uneingeschränktes Recht auf Kopien ihrer Daten. Gemäß Erwägungsgrund 63 kann der Verantwortliche um eine Präzisierung bitten (um nicht immer ALLE Daten kopieren zu müssen); doch die betroffene Person kann trotzdem ALLE Daten einfordern.

Dieser Pflicht wird das Kürzel **[GVO_015a]** zugeordnet (siehe Seite 14).

2.5.1 Allgemeine Informationen zur Pflicht [GVO_015a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 27 Abs. 2 BDSG und § 28 Abs. 2 BDSG **kein** Recht auf Datenkopie, sofern wissenschaftliche oder historische Forschungszwecke oder Statistikzwecke oder öffentliche Archivzwecke erfüllt werden. Auch der (umstrittene) § 34 Abs. 1 Nr. 2b BDSG hebt die Datenkopie-Pflicht auf, sofern die Daten u.a. nur zu Backup-Zwecken gespeichert sind; die Gründe der Auskunftsverweigerung sind zu nennen und zu dokumentieren. Der § 34 Abs. 2 Satz 3 BDSG fordert, dass die Daten zur Auskunftserteilung streng zweckgebunden und ansonsten wirksam eingeschränkt verarbeitet werden müssen (für andere Zwecke sind sie einzuschränken, siehe Pflicht **[GVO_018]** auf Seite 80).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.
• CR 05/2019 Seite 295-301 (diverse rechtliche Überlegungen).

[Im Rahmen des PrivazyPlan® wird das Dossier „Kopie (für die betroffene Person)“ 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.]

2.5.2 Was bedeutet diese Pflicht [GVO_015a] ?

a) Allgemeine Aspekte

ACHTUNG Baustelle:

Sämtliche Aspekte der „Datenkopie“ sind unter Experten umstritten und werden von Gerichten auf verschiedene Weise angewendet.
- Was bezweckt das Recht auf Datenkopie?
- Bedeutet jeder Wunsch nach Auskunft automatisch auch eine Kopie?
- Wie umfangreich/ausführlich muss die Kopie sein?

Die Rechtsunsicherheit ist enorm.

... bitte lesen Sie weiter. Auf den folgenden fünf Seiten haben wir die Struktur geändert und auch noch einige neue Quellen genannt. Inhaltlich wird dadurch nur noch klarer: Wir fischen alle im Trüben!

Das Recht auf „Datenkopie“ wurde durch die DS-GVO erstmals eingeführt.

Auch bei dieser stufenweise Vorgehensweise gilt die **Monatsfrist** des Artikel 12 (3). Insofern ist Eile geboten, weil die betroffene Person in diesem Zeitraum zufriedengestellt werden soll. Eine Fristverlängerung um bis zu zwei Monate kann gerechtfertigt sein, wenn auf Backups zugegriffen werden muss (oder wenn größere Mengen an Videomaterial gesichtet werden müssen).

Wenn das Unternehmen wirklich eine Komplett-Kopie an die betroffene Person ausliefern können will, so muss dies gründlich geplant werden. Diese Pflicht sollte daher möglichst früh bearbeitet werden (eine grobe Priorisierung der Pflichten findet sich auf Seite 19; ein exemplarischer Leitfaden findet sich auf Seite 358).

Dieses Recht darf nicht verwechselt werden mit dem „**Recht auf Datenübertragbarkeit**“ gemäß Artikel 20 (siehe Pflicht **[GVO_020]** auf Seite 88). Hier beim

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.6 Berichtigung ermöglichen [GVO_016]

Persönlichkeitsrechte

Gemäß Artikel 16 haben betroffene Personen das Recht auf eine Berichtigung von unrichtigen Daten. In der Datenverarbeitung ist ein Datenfeld aufzunehmen, wo die betroffene Person eine „ergänzende Erklärung“ hinterlegen kann (um den Kontext korrekt und unmissverständlich klarzustellen).

Dieser Pflicht wird das Kürzel **[GVO_016]** zugeordnet (siehe Seite 14).

2.6.1 Allgemeine Informationen zur Pflicht [GVO_016]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 27 Abs. 2 BDSG und § 28 Abs. 2 BDSG **keine** Berichtigungspflicht, sofern wissenschaftliche oder historische Forschungszwecke oder Statistikzwecke oder öffentliche Archivzwecke erfüllt werden.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

[Im Rahmen des PrivazyPlan® wird das Dossier „Berichtigung“ (8Treffer) 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.]

2.6.2 Was bedeutet diese Pflicht [GVO_016] ?

Eine ähnliche Regelung stellte § 35 Abs. 1 BDSG-alt dar. Die Pflicht zur Speicherung einer „ergänzenden Erklärung“ gab es im BDSG aber nur in Hinsicht auf Auskunfteien; jetzt trifft es jedes (!) Unternehmen.

Ist eine Berichtigung nicht möglich, so kann gemäß Artikel 5 (1d) eine Löschung notwendig sein. (Hierbei geht es also nicht um ein Löschen als Ganzes, sondern nur um die unrichtigen Details. Daher hat es nichts mit „Recht auf Vergessenwerden“ gemäß Artikel 17 zu tun.

Es müssen nur die „relevanten“ Daten berichtigt werden, wie Gola in RdNr. 4 und 12 zu Artikel 16 mit Verweis auf Artikel 5 (1d) argumentiert; so müsste beispielsweise die Postadresse eines Kunden, dessen Lieferung etc. abgeschlossen sei, nicht mehr berichtigt werden.

Diese Pflicht ist eng verbunden mit Artikel 19 („Mitteilungspflicht von Berichtigungen etc.“), siehe Pflicht **[GVO_019]** auf Seite 84.

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite 39).

2.6.3 Wie erfüllt man diese Pflicht [GVO_016] ?

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: ● Die Berichtigungs-Verlangen der betroffenen Personen müssen erfüllt werden. ● Eventuell sind sogar „ergänzende Erklärungen“ zu speichern. ● Externen Daten-Empfängern muss das Berichtigungs-Verlangen mitgeteilt werden. ● ➔ Nutzen Sie das Beispielformular von Seite 362.

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 24.

☐ Die betroffenen Personen haben ein Recht auf eine „**ergänzende Erklärung**“, um den Kontext (aus deren Sicht) korrekt und unmissverständlich klarzustellen. Hierfür benötigt man z.B. in Datenbanken ein eigenes Textfeld, welches dann an allen relevanten Stellen angezeigt werden, damit es seine Wirkung

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.7 Löschen aus betrieblichen Gründen [GVO_017]

Persönlichkeitsrechte

Im Artikel 17 (1) werden verschiedene betriebliche Gründe und Umstände für das Löschen von Daten beschrieben. Das Unternehmen muss demnach selbst laufend prüfen, ob es die Daten noch speichern darf, oder ob es diese unverzüglich löschen muss. Ein „versehentliches Liegenlassen“ von personenbezogenen Daten kann mit Geldbußen geahndet werden. [23]

Dieser Pflicht wird das Kürzel **[GVO_017]** zugeordnet (siehe Seite 14).

2.7.1 Allgemeine Informationen zur Pflicht [GVO_017]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) muss/darf gemäß § 35 BDSG eine „Einschränkung der Verarbeitung“ anstelle einer Löschung vorgenommen werden. Siehe Seite 288.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● VdS-Richtlinie 10010 (Seite 512) im dortigen Kapitel 14 („Datenmanagement“) ● In der Zeitschrift ZD 07/2017 wird auf Seite 314-319 sehr anschaulich beschrieben, wie schwierig das Löschen sein kann.

[Im Rahmen des PrivazyPlan® wird das Dossier „Löschung“ 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.]

2.7.2 Was bedeutet diese Pflicht [GVO_017] ?

Dieser Artikel stellt klar, wann ein Unternehmen ganz generell Daten löschen muss. Hierfür braucht es (auf den ersten Blick) keinerlei Interaktion mit den betroffenen Personen. Daten sind zu löschen, wenn…

1.) Gemäß Artikel 17 (1a), wenn der zugrundeliegende Zweck entfällt. Dies kann z.B. bei abgelehnten Bewerbern der Fall sein. Ähnlich zu § 35 Abs. 2 Nr. 3 BDSG-alt.
2.) Gemäß Artikel 17 (1d), wenn die Datenverarbeitung unrechtmäßig ist. Ähnlich zu § 35 Abs. 2 Nr. 1 BDSG-alt.
Der Kühling/Buchner-Fachkommentar fordert in RdNr. 17 zu Artikel 18, dass die betroffene Person auf ihr Recht zur „Einschränkung der Verarbeitung statt Löschung“ hingewiesen werden muss (und sie demnach eine Einschränkung statt Speicherung fordern könne); siehe Seite 81. [24]
3.) Gemäß Artikel 17 (1e), wenn die Löschung durch Gesetze bzw. Verordnungen geboten ist.

Demzufolge muss das Unternehmen seine Datenbestände kontinuierlich darauf prüfen, ob eine Löschung notwendig ist.

[Anmerkung: Der Artikel 17 (1) fordert außerdem Löschungen nach Widerspruch bzw. Widerruf (siehe Seite 95 und Seite 149); siehe Löschkonzept auf Seite 364.]

Unabdingbar für die Erfüllung dieser Pflicht ist eine präzise Festlegung der Löschfristen im Verarbeitungsverzeichnis gemäß Artikel 30 (1f). Für jede Datenkategorie einer Verarbeitung muss die Löschfrist spezifiziert werden (siehe Kapitel 13.7 auf Seite 550).

Ganz am Rande erwähnt: Eine Lösch- (bzw. Berichtigungs-) Pflicht ergibt sich auch aus Artikel 5 (1d), wenn die Daten unrichtig sind. Das Lösch-Verlangen ist eng verbunden mit Artikel 19 („Mitteilungspflicht von Berichtigungen etc.“, siehe Seite 84).

[23] Der Artikel 17 (1) ist im ersten Satz etwas unglücklich formuliert. Dort werden zwei völlig verschiedene Sachverhalte in einem Satz mit einem „und“ verknüpft. Die dann folgenden Kriterien in den Literalen a-f wirken ebenfalls willkürlich gewürfelt und bringen keine Klarheit. Diese Vermischung wird aufgehoben, indem hier im Rahmen von PrivazyPlan® zwei verschiedene Pflichten formuliert werden.

[24] Das BAG hat entschieden: Wenn Arbeitgeber/-innen die betriebliche Mitbestimmung umgehen und personenbezogene Daten verarbeiten, dann darf der Betriebsrat dies zwar stoppen, aber keine Löschung verlangen. Der 29-seitige Beschluss nimmt aber fast keinen Bezug auf das Datenschutzrecht (Az. 1 ABR 31/19 vom 23.03.2021). Siehe Datenschutz-Berater 02/2022 auf Seite 64-65.

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.8 Löschen auf Verlangen der betroffenen Person [GVO_017a]

Persönlichkeitsrechte

Im Artikel 17 (1) kann die Löschung von Daten durch eine betroffene Person verlangt werden. [23]

Dieser Pflicht wird das Kürzel **[GVO_017a]** zugeordnet (siehe Seite 14).

2.8.1 Allgemeine Informationen zur Pflicht [GVO_017a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

[Im Rahmen des PrivazyPlan® wird das Dossier „Löschung“ 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.]

2.8.2 Was bedeutet diese Pflicht [GVO_017a] ?

a) Wann kann eine Person das Löschen verlangen?

In Bezug auf ein Lösch-Verlangen kommen die folgenden drei Literale in Frage:

1.) Gemäß Literal „b“, wenn sie auf einer Einwilligung beruhen und diese widerrufen wird (und keine andere Rechtsgrundlage dem gegenübersteht).
2.) Gemäß Literal „c“, wenn die betroffene Person Widerspruch einlegt und der Verantwortliche keine vorrangig berechtigten Gründe aufweisen kann. Dies zielt auf die „berechtigten geschäftlichen Interessen“ des Verantwortlichen gemäß Artikel 6 (1f) ab.
3.) Gemäß Literal „f“, wenn die Daten von Kindern gespeichert sind und diese gelöscht werden sollen. (Diese Interpretation stammt von Paal/Pauly in Rdnr. 28 zu Artikel 16.)

Wenn man dies wörtlich nimmt, dann löst der obige Widerspruch bzw. Widerruf selbst noch keine Löschpflicht aus. Vielmehr muss die betroffene Person dies explizit verlangen (in diesem Sinne gedeutet von Paal/Pauly in RdNr. 34 zu Artikel 17). Diese Denkweise entspräche dem BDSG-üblichen Denkansatz: Der reine Widerruf einer Einwilligung gilt nur für die Daten der Zukunft (und nicht rückwirkend).

b) Wann kann ein Lösch-Verlangen abgelehnt werden?

Zahlreiche Ausnahmen liefert der Artikel 17 (3), wodurch ein Löschverlangen abgelehnt werden kann.

Besonders hervorzuheben ist die Ausnahme gemäß Artikel 17 (3b); demnach kann ein Löschverlangen abgelehnt werden, wenn die Verarbeitung zur „Erfüllung rechtlicher Verpflichtungen“ gemäß Artikel 6 (1c) dient. Dies wäre z.B. bei steuerlichen Aufbewahrungsfristen gegeben.

Siehe RDV 02/2018 Seite 70-75. Weitere Details in Kühling/Buchner (2. Auflage, RdNr. 75 zu Artikel 17).

c) Sonstiges

Das „Spickmich“-Urteil des BGH (Az. VI ZR 196/08 vom 23.06.2009) zeigte auf, wie schwierig das Löschbegehren zu bewerten ist. Auch das „Google Spain“-Urteil des EuGH (C-131-/12 vom 13.05.2014) zeigt die hohe Komplexität der Fragestellung.

Die betroffenen Personen sind über ihre Lösch-Rechte zu informieren, wie Artikel 13 (2b) und Artikel 14 (2c) festlegen. Auch im Rahmen des allgemeinen Auskunftsrechts gemäß Artikel 15 (1e) müssen der betroffenen Person die Löschrechte mitgeteilt werden.

Das „Recht auf Vergessenwerden“ im Sinne des Artikel 17 (2) findet nur dann Anwendung, sofern die betroffene Person einen entsprechenden Antrag stellt (siehe folgendes Kapitel 2.9).

⚠ Eine **unterlassene Löschung** wird zum massiven Problem, wenn es um die Aushändigung einer Datenkopie gemäß der Pflicht **[GVO_015a]** an die betroffene Person geht (siehe Seite 66).

Diese Pflicht ist eng verbunden mit Artikel 19 („Mitteilungspflicht von Berichtigungen etc.“), siehe Pflicht **[GVO_019]** auf Seite 84.

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.9 Löschen veröffentlichter Daten („Recht auf Vergessenwerden“) [GVO_017b]

Persönlichkeitsrechte

Gemäß Artikel 17 (2) kann eine betroffene Person in Bezug auf „Veröffentlichungen“ das Löschen von Daten oder Links verlangen. Dies entspricht dem „Digitalen Radiergummi“. Hat das Unternehmen personenbezogene Daten z.B. per Bewertungsportal oder Suchmaschine etc. veröffentlicht, so muss es jene Dienste auf den Löschantrag der betroffenen Person hinweisen (sofern dies zumutbar ist).

Bitte verwechseln Sie diese Pflicht nicht mit [GVO_019] auf Seite 84, welche dann greift, wenn Sie personenbezogene Daten an ganz bestimmte Dritte zu ganz bestimmten Zwecken weitergeben. Bei der hiesigen Pflicht geht es um „diffuse“ Offenlegungen in Suchmaschinen und Bewertungsportalen etc.

Dieser Pflicht wird das Kürzel **[GVO_017b]** zugeordnet (siehe Seite 14).

2.9.1 Allgemeine Informationen zur Pflicht [GVO_017b]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) bestehen gemäß § 35 Abs. 1 BDSG zwei Ausnahmen von der Löschpflicht:
1.) bezüglich nicht-automatisierter Datenverarbeitungen in Form von Karteikarten oder handschriftlicher Listen (siehe Seite 613), wo eine Löschung aufgrund der besonderen Art der Speicherung nicht möglich ist, und
2.) bezüglich automatisierter Datenverarbeitungen, wo die Löschung nur mit unverhältnismäßig hohem Aufwand möglich ist (siehe Pflicht **[BDSG_035]** auf Seite 288),
aber in beiden Fällen nur dann, wenn
1.) das Lösch-Interesse der betroffenen Person als gering anzusehen ist und

2.) die Verarbeitung an sich rechtmäßig war, wie es Artikel 17 (1d) thematisiert,

was dann zu dem Ergebnis führt, dass der Verantwortliche nicht löschen muss, sondern er die Verarbeitung nur einschränken darf (siehe Artikel 18 und Pflicht **[GVO_018]** auf Seite 80). Ähnlich § 35 Abs. 3 Nr. 3 BDSG-alt. [27]

Im BDSG (in der Fassung ab dem 25.05.2018) liefert der deutsche Gesetzgeber mit § 35 Abs. 2 BDSG eine Regelung von bizarrer Komplexität, die trotz Gesetzesbegründung sehr kryptisch ist. Vermutlich ist Folgendes gemeint: Sollte der Verantwortliche einen konkreten Grund zur Annahme haben, dass ein Löschen von Daten (z.B. nach Erreichen der 10-jährigen Löschfrist hinsichtlich steuerlicher Aufbewahrungspflichten, siehe Kapitel 13.7 auf Seite 550) das schutzwürdige Interesse einer betroffenen Person beeinträchtigt, so sollte statt dessen nur die Verarbeitung eingeschränkt werden. Ähnlich § 35 Abs. 3 Nr. 2 BDSG-alt.
Die betroffene Person soll möglichst darüber informiert werden, damit sie dann entscheiden kann, ob eine Löschung wirklich erfolgen soll. Dies wird in der Pflicht **[BDSG_035]** im Kapitel 10.7 auf 288 beschrieben

Im BDSG (in der Fassung ab dem 25.05.2018) liefert der deutsche Gesetzgeber mit § 35 Abs. 3 BDSG eine Regelung von bizarrer Komplexität, die trotz Gesetzesbegründung sehr kryptisch ist. Die bereits in Artikel 17 (3b) bestehende Lösch-Ausnahme wird nun ergänzt durch den Umstand, dass der Verantwortliche satzungsgemäße oder vertragliche Aufbewahrungsfristen zu beachten hat (siehe Seite 291).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● DSK-Kurzpapier-11 ● Zeitschrift ZD 12/2015 Seite 570-577.

2.9.2 Was bedeutet diese Pflicht [GVO_017b] ?

Die hier in der DS-GVO gewählte Formulierung des „Öffentlich-Machens“ ist nirgendwo definiert (wie bei allen anderen Begriffen des Datentransfers auch). Ein Erklärungsversuch findet sich im Kapitel 13.5 auf Seite 539. Die Fachautoren sind sich einig, dass es um eine Offenbarung an einen „unbestimmten Personenkreis“ geht (ohne Beispiele zu nennen).

[27] Ja, die Komplexität dieser Regelung ist enorm. Ohne die (kryptische und unvollständige) Gesetzesbegründung hätte sich der Sinn wohl überhaupt nicht vollständig erschlossen. Für den normalen Rechtsanwender sind die Formulierungen des § 35 BDSG (mitsamt Gesetzesbegründung) eine absolute Zumutung.

2.10 Einschränkung der Verarbeitung [GVO_018]

Persönlichkeitsrechte

Gemäß Artikel 18 (1) können betroffene Personen unter bestimmten Umständen eine „Einschränkung der Verarbeitung“ verlangen; oftmals wird dies auch als „Sperrung“ bezeichnet. Der Sinn dieser „Einschränkung“ liegt darin, dass in verschiedenen Streitfällen die Daten erst einmal „eingefroren“ werden, bis eine Klärung der Sachlage erfolgt ist.

Dieser Pflicht wird das Kürzel **[GVO_018]** zugeordnet (siehe Seite 14).

2.10.1 Allgemeine Informationen zur Pflicht [GVO_018]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Es gibt auch noch eine völlig andere Ausprägung eines „Rechts auf Einschränkung“, worauf hier der Vollständigkeit halber hingewiesen werden soll. Unter bestimmten Umständen darf ein Verantwortlicher die Verarbeitung lediglich einschränken, statt die Daten löschen zu müssen. Siehe Seite 77 und siehe Pflicht **[BDSG_035]** auf Seite 288.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente. Siehe DatenschutzPraxis 06/2017 Seite 6-7.

Die Fachliteratur ist notwendig, weil diese Regelung sehr komplex ist. Es ist dringend angeraten die Fachliteratur zu konsultieren, weil die gesamte Komplexität hier im PrivazyPlan® nicht wiedergegeben werden kann.

[Im Rahmen des PrivazyPlan® wird das Dossier „Einschränkung der Verarbeitung“ 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.]

2.10.2 Was bedeutet diese Pflicht [GVO_018] ?

a) Was meint die DS-GVO mit „Einschränkung“?

Gemäß Artikel 4 Nr. 3 können Daten markiert werden, um deren Verarbeitung kurzzeitig einzuschränken (engl. „restriction of processing“). [28] Die Beschäftigten können anhand einer solchen Markierung erkennen, dass diese Daten nicht genutzt bzw. geändert oder gelöscht werden dürfen. Man könnte dies auch umschreiben als „sperren“, „pausieren“, „einfrieren“, „verdecken“, „verstecken“, „deaktivieren“ oder „temporär löschen“; oder als „Zweckbegrenzung zugunsten der betroffenen Person“.

Sogar eine Nutzung der Daten durch den Verantwortlichen wie z.B. zu Zwecken der Verteidigung gegen Rechtsansprüche ist gemäß Artikel 18 (2) nur mit Einwilligung zulässig.

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite 39).

b) Wann muss die Verarbeitung eingeschränkt werden?

Es gibt vier Szenarien:

a) Die betroffene Person **bestreitet die Richtigkeit der Daten** gemäß Artikel 18 (1a). Dafür muss sie keine Beweise oder auch nur Nachweise liefern. Das einfache Bestreiten reicht aus. Siehe den Beschluss des VG Stade mit Az. 1 B 1918/18 vom 09.10.2018. Der Verantwortliche muss die Datenverarbeitung einschränken und die Richtigkeit der Daten prüfen. Sind die Daten korrekt, so darf der die Verarbeitung fortführen (nachdem er die betroffene Person informiert hat). Andernfalls müssen die Daten wohl gelöscht werden, denn die DS-GVO äußert sich zu diesem Szenario nicht und dann wäre das Löschen die einzige Konsequenz (siehe Wikipedia zu „non liquet“).
Angesichts dieser Umstände sollte ein Verantwortlicher die Daten stets so erheben, dass er deren Richtigkeit stets beweisen kann (also beispielsweise

[28] Leider wird das englische „restriction“ an anderer Stelle als „Beschränkung“ übersetzt und hat – z.B. im Artikel 5 (1c) hinsichtlich der Datenminimierung – eine ganz andere Bedeutung. Im Erwägungsgrund 67 werden beide Übersetzungen parallel genutzt und sorgen für Verunsicherung. Leider gibt es im Englischen auch ein „limitation of processing“, welches ebenfalls als „Beschränkung“ übersetzt wurde; dies bezieht sich aber auf andere Zusammenhänge (siehe Dossier „Untersagung“).

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.11 Korrektur bei Dritten (Nachberichtigung) [GVO_019]

Persönlichkeitsrechte

Gemäß Artikel 19 muss sich jede Forderung nach Berichtigung, Löschung oder Verarbeitungseinschränkung möglichst auf die gesamte Datenkette beziehen (in Bezug auf die Artikel 16, Artikel 17 (1) und Artikel 18). Über dieses Verlangen der betroffenen Person sind Auftragsverarbeiter und Dritte darüber zu informieren. Die betroffene Person kann außerdem verlangen, dass die Namen der Empfänger genannt werden (um kontrollieren zu können, ob die Daten insgesamt bei allen Beteiligten korrekt gehandhabt werden).

Bitte verwechseln Sie diese Pflicht nicht mit [GVO_017b] auf Seite 77, welche als „digitaler Radiergummi“ dann greift, wenn Sie personenbezogene Daten ganz „diffus“ in Suchmaschinen und Bewertungsportalen etc. offenlegen. Hier bei [GVO_019] geht es um Offenlegungen an ganz bestimmte externe Empfänger zu ganz bestimmten Zwecken.

Dieser Pflicht wird das Kürzel **[GVO_019]** zugeordnet (siehe Seite 14).

2.11.1 Allgemeine Informationen zur Pflicht [GVO_019]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

2.11.2 Was bedeutet diese Pflicht [GVO_019] ?

a) Voraussetzung: Die betroffene Person fordert bestimmte Rechte ein

Die Voraussetzung besteht zunächst darin, dass eine betroffene Person ihre diesbezüglichen **Rechte einfordert**.

Dies sind die Rechte auf:

- Berichtigung gemäß Artikel 16 und Pflicht **[GVO_016]** auf Seite 70.
- Löschung gemäß Artikel 17 (1) und Pflicht **[GVO_017a]** auf Seite 75.
- Verarbeitungseinschränkung gemäß Artikel 18 und Pflicht **[GVO_018]** auf Seite 80.

In diesen drei Fällen muss also das jeweilige Verlangen der betroffenen Person erfüllt werden; darüber hinaus besteht gemäß der hier thematisierten Pflicht **[GVO_019]** ein zusätzlicher Handlungsbedarf: Die „Nachberichtigung“.

Diese Pflicht gilt erst ab dem 25.05.2018. Alle zuvor getätigten Offenlegungen sind nicht betroffen.

Es sind die Fristen zu berücksichtigen, die gemäß Artikel 12 (3) festgelegt sind (also „unverzüglich“, spätestens aber innerhalb von einem Monat, siehe Seite 39).

b) Voraussetzung: Die Daten müssen zuvor „offengelegt“ worden sein

Diese Pflicht kommt nur dann zum Tragen, wenn der Verantwortliche die Daten zuvor „offengelegt“ hat. Der Begriff „**Offenlegung**“ ist jedoch nicht definiert. Im Kapitel 13.5 auf Seite 530 („Daten-Transfer – ein Merkblatt“) wird ein Versuch unternommen, diesen Begriff zu verstehen. Demnach gilt diese Pflicht für drei Fälle:

- die Daten wurden an Empfänger innerhalb der EU/EWR übermittelt,
- die Daten wurden an Empfänger in Drittländern bzw. internationalen Organisationen übermittelt,
- die Daten werden im Auftrag durch einen Dienstleister verarbeitet.

b) Es bedarf einer Liste aller Daten-Empfänger

Damit das Verlangen der betroffenen Person weitergeleitet werden können, muss der Verantwortliche zuvor die potenziellen Empfänger dokumentiert haben.
Demnach muss es für jede einzelne Verarbeitung eine Liste der oben genannten Daten-Empfänger geben. Idealerweise lässt sie sich dem Verarbeitungsverzeichnis gemäß Artikel 30 und der Pflicht **[GVO_030]** entnehmen (siehe Seite 110). Dies wären beispielsweise:

- Finanzamt, Krankenkasse, Steuerberater, Auskunftei, …
- Internationale Fluggesellschaften, …
- IT-Dienstleister, Druckerei, Lohnbüro, …

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.12 Datenübertragbarkeit ermöglichen [GVO_020]

Persönlichkeitsrechte

Betroffene Personen haben gemäß Artikel 20 das Recht, dass die von ihnen bereitgestellten Daten exportiert (und zu einem Konkurrenz-Anbieter übertragen) werden können. Dies betrifft nur die automatisierten Verarbeitungen, die auf einem Vertragsverhältnis oder einer Einwilligung beruhen. Dieses Recht darf nicht verwechselt werden mit dem „Recht auf Kopie“ gemäß Artikel 15 (3) (siehe Seite 70).

Dieser Pflicht wird das Kürzel **[GVO_020]** zugeordnet (siehe Seite 14).

2.12.1 Allgemeine Informationen zur Pflicht [GVO_020]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 28 Abs. 2 BDSG **kein** Recht auf Übertragbarkeit, sofern öffentliche Archivzwecke erfüllt werden.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● ZD 05/2019 Seite 191-194 (klammert Nutzungsdaten aus) ● PinG 01/2019 Seite 13-21 ● Datenschutz-Berater 05/2019 Seite 96-98 ● PinG 06/2018 Seite 239-243 ● In der ZD 11/2018 auf Seite XV-XVII wird das Thema zusammengefasst. ● RDV 02/2018 Seite 80-85 ● 264-seitige Studie „Datenportabilität“ der Stiftung Datenschutz (die auf Seite 42 auch keine Hilfe ist, wenn es um die zentrale Fragestellung der „Bereitstellung“ geht). Ab Seite 57 in Englisch. Es gibt auch eine Kurzversion. ● DatenschutzPraxis 07/2017 Seite 1-3 ● ZD 08/2017 Seite 355-361 (Was bedeutet „bereitstellen“ der Daten?) ● Siehe Beck'scher Online Kommentar von Paal/Pauly. ● Das Workingpaper „WP 242“ mitsamt FAQ der Artikel-29-Datenschutzgruppe ● PinG 01/2017 Seite 5-8.

[Im Rahmen des PrivazyPlan® wird das Dossier „Datenübertragbarkeit“ (6 Treffer) 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.]

2.12.2 Was bedeutet diese Pflicht [GVO_020] ?

Wenn das Unternehmen wirklich einen maschinenlesbaren Datenexport an die betroffene Person ausliefern können will, so muss dies gründlich geplant werden. Diese Pflicht sollte daher möglichst früh bearbeitet werden (eine grobe Priorisierung der Pflichten findet sich auf Seite 19).

Dieses Betroffenenrecht soll wohl die Marktmacht von Facebook etc. brechen, indem die Nutzerdaten nicht länger „eingesperrt“ sind. Insofern wollte Brüssel wohl den Wechsel zu datenschutzfreundlichen Anbietern erleichtern.

Google zeigt mit „**Google Takeout**“, wie es geht. Siehe auch hier und hier. Innerhalb weniger Minuten erhält man eine ZIP-Datei mit Daten, die Google gespeichert hat. Derzeit sind noch nicht alle Google-Dienste abgedeckt, aber das ist wohl nur eine Frage der Zeit. Auch **facebook** bietet wohl schon eine Export-Funktion an (siehe hier). [29]

Es gelten die folgenden Einschränkungen:

- Relevant sind nur jene Daten, die die betroffenen Personen **selbst bereitgestellt** haben (im Sinne des Artikel 13). Das Unternehmen muss also z.B. die Stamm- und ggf. die Nutzungsdaten bereitstellen. Irrelevant sind Daten, die bei Dritten erhoben wurden (im Sinne des Artikel 14). Wurden die Daten hingegen bei Auftragsverarbeitern bereitgestellt, so unterliegen diese natürlich der Pflicht zur Datenübertragbarkeit.

  Was ist eine „Bereitstellung“ von Daten, die zum Recht auf Datenübertragbarkeit führt? Sind nur jene Daten relevant, welche die betroffene Person durch bewusstes Handeln liefert? Unstrittig betroffen sind jene Daten, die eigenhändig per Tastatur eingetippt wurden. Was aber ist mit Logfiles, die versteckt im Hintergrund erzeugt werden? Was ist mit den Videodaten, die entstehen, wenn sich eine Person im Sichtfeld einer Videokamera befindet? Was ist mit den Geo-Daten einer Fitness-Uhr, die an den Anbieter übertragen werden?

  Man beachte den Unterschied zum Wortlaut des Artikel 15 (3), wo eine Ko-

[29] Unter anderem finden sich im Export auch zahlreiche Positionsdaten, deren Datum im Unixformat gespeichert werden. Die Umrechnung gelingt Ihnen in MS-Excel folgendermaßen: =DATUM(1970;1;1)+(LINKS(A1;10)/86400) und die Zelle als "Datum" formatieren

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.13 Widerspruchsrecht einräumen [GVO_021]

Persönlichkeitsrechte

Gemäß Artikel 21 kann eine betroffene Person einer Verarbeitung widersprechen, sofern die Rechtsgrundlage der Verarbeitung auf **(a)** öffentlichen Interessen oder **(b)** berechtigten Unternehmensinteressen beruht. Die Person muss „eine besondere Situation“ nachweisen. Das Unternehmen kann dies ablehnen, wenn die Verarbeitung zwingend notwendig ist.

Dieser Pflicht wird das Kürzel **[GVO_021]** zugeordnet (siehe Seite 14).

2.13.1 Allgemeine Informationen zur Pflicht [GVO_021]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

[Im Rahmen von PrivazyPlan® wird das Dossier „Widerspruch“ 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.]

2.13.2 Was bedeutet diese Pflicht [GVO_021] ?

a) Wogegen kann eine betroffene Person widersprechen?

In den folgenden Szenarien kann eine Person der Datenverarbeitung widersprechen:

- Gegen Verarbeitungen, deren Wahrnehmung gemäß Artikel 6 (1e) im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt. Eine „besondere Situation“ muss vorliegen, und es dürfen keine zwingenden Gründe des Verantwortlichen entgegenstehen.

- Gegen Verarbeitungen, die gemäß Artikel 6 (1f) zur **Wahrung berechtigter Interessen** des Verantwortlichen erforderlich sind. Eine „besondere Situation“ muss vorliegen, und es dürfen keine zwingenden Gründe des Verantwortlichen entgegenstehen. Dies gilt auch im Rahmen des „Konzernprivilegs“ (siehe Seite 553).

- Gegen **Direktwerbung** (siehe Seite 271), also gegen jede Werbung z.B. per Brief, Telefon und E-Mail. Die DS-GVO geht leider kaum auf den Begriff „Direktwerbung“ ein. Im Erwägungsgrund 47 wird sie als „berechtigtes Interesse“ angesehen. Insofern unterliegt sie eigentlich dem obigen Punkt. Doch hinsichtlich der Direktwerbung wird keine „besondere Situation“ des Betroffenen vorausgesetzt. Insofern handelt es sich hier um ein bedingungsloses Widerspruchsrecht. Der Artikel 21 (3) bekräftigt dies, indem ein sofortiger Verarbeitungsstop gefordert wird.

- Bei **Internet-Diensten** kann gemäß Artikel 21 (5) ein Widerspruch durch technische Konfigurationen verlangt werden (z.B. „do-not-track“ im Webbrowser).

- Gegen wissenschaftliche und historische **Forschungszwecke** oder zu statistischen Zwecken. Eine „besondere Situation“ muss vorliegen, und es dürfen keine erforderlichen öffentlichen Interessen entgegenstehen.

  Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 27 Abs. 2 BDSG und § 28 Abs. 2 BDSG **kein** Widerspruchsrecht (bzw. nicht in vollem Umfang), sofern wissenschaftliche oder historische Forschungszwecke oder Statistikzwecke oder öffentliche Archivzwecke erfüllt werden. Ein Widerspruch darf diese Zwecke nicht unmöglich machen.

Was ist eine „besondere Situation“? Die DS-GVO erklärt dies nicht. Es sind wohl individuelle und konkrete Gründe, die nachvollziehbarer Weise von subjektiver Wichtigkeit sind. Derlei Gründe muss die betroffene Person nachweisen und mit Tatsachen begründen können, und einer Prüfung mit strengen Maßstäben standhalten können. Denkbar sind rechtliche, wirtschaftliche, ethische, soziale, gesellschaftliche oder familiäre Zwangssituationen bzw. eine Gefahr für Leib, Leben oder Vermögen der betroffenen Person. Konkrete Anhaltspunkte werden die Aufsichtsbehörden und Gerichte liefern.

Praktisch gesehen ist meistens der Widerspruch gegen Direktwerbung relevant. Hier werden möglicherweis nationale Regelungen berührt (in Deutschland beispielsweise der § 7 UWG).

[Ab hier eine Lücke aufgrund der Leseprobe...]

2.14 Automatisierte Entscheidung vermeiden [GVO_022]

Persönlichkeitsrechte

Gemäß Artikel 22 darf eine Person nicht einer voll automatisierten Entscheidung (bzw. Profiling im Sinne des Artikel 4 Nr. 4) unterworfen werden, wenn daraus erhebliche Nachteile für sie erwachsen. Stattdessen muss immer auch ein Mensch an solchen Entscheidungen beteiligt werden.

Dieser Pflicht wird das Kürzel **[GVO_022]** zugeordnet (siehe Seite 14).

2.14.1 Allgemeine Informationen zur Pflicht [GVO_022]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5b) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im BDSG (in der Fassung ab dem 25.05.2018) besteht gemäß § 37 Abs. 1 BDSG eine Ausnahme: Bei Versicherungsverträgen kann im Falle einer Leistungserbringung durchaus eine automatisierte Einzelfallentscheidung erlaubt sein.

In der **Fachliteratur** (siehe Seite 518) gibt es sehr ausführliche Kommentare zu diesem Artikel 22. Das ist auch notwendig, weil die Details zur automatisierten Einzelfallentscheidung sehr vielfältig sind. Es ist dringend angeraten die Fachliteratur zu konsultieren, weil die gesamte Komplexität hier im PrivazyPlan® nicht wiedergegeben werden kann.
Konkret sind die folgenden Quellen interessant: ● „Ethik für Algorithmen“ in c’t 08/2020 Seite 74-77 ● PinG 01/2019 Seite 1-4 ● Der Datenschutz-Berater 12/2018 berichtet ausführlich auf Seite 253-255 ● Das Workingpaper „WP 251 rev01“ in deutscher Sprache ● „Zeitschrift für Datenschutz“ 06/2018 auf Seite 304-307 ● Datenschutz-PRAXIS 03/2018 Seite 8-11 ● Datenschutz-Berater 02/2018 Seite 35-37 ● RDV 01/2017 Seite 3-9 ● Zeitschrift c’t 25/2017 Seite 68-70 mit Berichten über Software in den USA, die den Richtern die Höhe von Haftstrafen empfiehlt.
Ansonsten noch interessant: Die Artikel-29-Datenschutzgruppe hat am 03.10.2017 das Workingpaper „WP 251“ zur Diskussion gestellt.

[Im Rahmen von PrivazyPlan® wird das Dossier „Automatisierte Entscheidung im Einzelfall“ 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.]

2.14.2 Was bedeutet diese Pflicht [GVO_022] ?

Die folgenden Aspekte sind wichtig:

- Die Verweigerung eines Vertragsabschlusses durch Anbieter aus monopolartigen Strukturen der Daseinsfürsorge (Gas, Wasser, Strom, ÖPNV, …) wäre eine erhebliche Beeinträchtigung.
- Die voll-automatisierte Kündigung von bestehenden Verträgen kann unter Umständen eine erhebliche Beeinträchtigung darstellen.
- Die Entscheidungen müssen nicht zwangsweise eine Totalablehnung oder -Verweigerung bedeuten; auch eine nur *teilweise* begünstigende Entscheidung kann erheblich beeinträchtigen.
- Die automatisierte Entscheidung muss schon ein Mindestmaß an Komplexität haben. Somit fällt ein biometrisches Zutrittssystem nicht unter den Artikel 22.

Der Artikel 22 (1) setzt voraus, dass **erhebliche** (vertragliche) Nachteile entstehen könnten. Dies ist eine sehr weiche Formulierung, die der Erwägungsgrund 71 auch nur geringfügig erhellt. Eine objektive Einschätzung der Sachlage mit Augenmaß bieten die Kommentare von Gola (RdNr. 22), Ehmann/Selmayr (RdNr. 9) und Kühling/Buchner (RdNr. 26). [31] Auch bei dieser Fragestellung zeigt, sich: Die Fachleute sind sich in mancher Hinsicht nicht einig. Man muss recht ausführlich die Fachliteratur konsultieren.

Der Artikel 22 (2) liefert verschiedene Gründe, warum eine automatisierte Einzelfallentscheidung doch rechtmäßig sein kann.

Der Artikel 22 (3) gibt den betroffenen Personen die Möglichkeit, den automatisierten Entscheidungsprozess zu verstehen und ggf. Einfluss zu nehmen.

[31] Manche Fachautoren wittern schon eine „erhebliche Benachteiligung“, wenn im Onlineshop die Zahlung per Rechnung verweigert wird. Hierbei wird oft die persönliche Meinung eines Rechtsreferendars in der ZD 02/2015 Seite 69 Bezug genommen (der seine Auffassung nicht explizit begründet). Auch sonst liefern die Befürworter keine Sachargumente. Soll man deswegen eine Datenschutz-Folgenabschätzung vornehmen, die dann vorgeschrieben wäre? Das ist doch absurd.

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 allein schon deswegen eine Geldbuße.

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*“ (engl. „Accountability“). 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 14).

3.1.1 Allgemeine Informationen zur Pflicht [GVO_005]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

⚠ Die in diesem Kapitel beschriebene Pflicht **[GVO_005]** hängt sehr eng zusammen mit der „weichen“ Pflicht **[AUX_008]**, die auf Seite 323 beschrieben wird. Wo ist der Unterschied?
Hier in der Nachweis-Pflicht **[GVO_005]** geht es „nur“ um einen schriftlichen Nachweis von fünf speziellen Themenbereichen. Es müssen also „nur“ ein paar Seiten Papier gefüllt werden.
Bei der „weichen“ Pflicht **[AUX_008]** geht es hingegen um alle Pflichten und deren vollständige Erfüllung durch den Einsatz eines Datenschutz-Managementsystems wie z.B. die VdS-Richtlinie 10010. Jene Pflicht geht also viel, viel weiter.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Ein bemerkenswerter Artikel in der „Zeitschrift für Datenschutz“ 01/2018 erörtert auf Seite 9-16 sehr ausführlich die Frage nach der notwendigen Ausführlichkeit der Pflicht zur „Accountability“. ● Die 19-seitige GDD-Praxishilfe DS-GVO IX (v2) („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] ?

a) Welche Bedeutung hat der Begriff „Rechenschaftspflicht“?

Leider wird der Begriff „Rechenschaft“ im Artikel 4 nicht definiert. Letztlich handelt es sich um einen unbestimmten Rechtsbegriff. Interessante Aspekte finden sich aber bei Wikipedia im lesenswerten Kapitel der Organisationslehre:

„Verantwortung beinhaltet in der Organisationslehre die Verpflichtung eines Stelleninhabers oder Funktionsträgers, über die ordnungsgemäße Erfüllung der seiner Stelle im Wege der Delegation übertragenen Aufgaben Rechenschaft abzulegen. **Verantwortung ist untrennbar mit Rechenschaft verbunden, Rechenschaft ist mithin kommunizierte Verantwortung. […]**
Rechenschaft bedeutet hier, dass der Funktionsträger über seine Aufgabenwahrnehmung an seinen Vorgesetzten oder an andere berichten muss und bei Fehlern sich den dafür vorgesehenen Sanktionen zu unterwerfen hat.“

b) Was umfasst die Rechenschaftspflicht in der DS-GVO?

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 21).

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

- Rechtmäßigkeit und Transparenz (siehe Seite 502 zum Thema „**Compliance**“)
- Zweckbindung (siehe auch „Zweckänderung“ auf Seite 46)
- Datenminimierung (siehe Seite 600)
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Diese hier vorliegende Rechenschaftspflicht hat natürlich große Schnittmengen mit den anderen ca. 50 Pflichten der DS-GVO (insbesondere **[AUX_008]** auf

[Ab hier eine Lücke aufgrund der Leseprobe...]

3.2 Datenschutzfreundliche Technikgestaltung und Voreinstellungen [GVO_025]

Dokumentation und Nachweis

Gemäß Artikel 25 (1) und Artikel 25 (2) muss der Verantwortliche schon in der Konzeptionsphase für Datenschutz sorgen, indem er so wenig Daten wie möglich speichert. Je weniger Daten er speichert, desto weniger Maßnahmen sind später zu deren Schutz notwendig (das spart Zeit und Geld). Ganz wichtig ist auch: Für jede Information, die man nicht besitzt, muss man später keine Auskunft erteilen oder Berichtigungsverlangen bearbeiten etc. (das spart Zeit und Nerven).

Dieser Pflicht wird das Kürzel **[GVO_025]** zugeordnet (siehe Seite 14).

3.2.1 Allgemeine Informationen zur Pflicht [GVO_025]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: • Das EDPB (siehe Seite 599) hat am 20.10.2020 einen EDPB-Guideline 2019-04 zu „Data Protection by Design and by Default“ veröffentlicht (die deutsche Übersetzung steht ab dem 13.04.2021 zur Verfügung) • Die Zeitschrift ZD 07/2017 berichtet auf Seite 308-313 sehr ausführlich.

Auf einen deutschen **Übersetzungsfehler** weist Marit Hansen in den BvD-News 02/2017 Seite 9 hin: Im Artikel 25 (2) findet sich im ersten Satz das Wort „*grundsätzlich*“. Dies ist in keiner anderen Sprache enthalten. Frau Hansen weist darauf hin, dass dieses Wort fälschlicherweise zu einem Verständnis führen könnte, dass es irgendwelche Ausnahmen geben könne.

3.2.2 Was bedeutet diese Pflicht [GVO_025] ?

Diese Pflicht wird im Kapitel 3 („Pflichten zu Dokumentationen und Nachweisen“) geführt, weil Erwägungsgrund 78 besagt:

> *„… Um die Einhaltung dieser Verordnung **nachweisen** zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun…“*

Dieser Artikel 25 liefert zwar nur ziemlich unbestimmte Forderungen, doch da er bei den Geldbußen im Artikel 83 (4a) genannt ist, wird er hier als explizite Pflicht behandelt. Ein Unternehmen kann es sich schlichtweg nicht leisten, diese Grundsätze zu ignorieren (daher sollte es möglichst nur zertifizierte Produkte anschaffen, siehe unten).

Wieso hat Brüssel diese Grundsätze mit so hohen Geldbußen versehen? Möglicherweise soll dies ein Zeichen in Richtung der großen US-Softwarehersteller sein (Facebook, Google, Microsoft, Apple, …), dass ein „Laissez-faire“ zukünftig sehr teuer werden kann. Der Erwägungsgrund 78 besagt:

> *„… In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten […] sollten die Hersteller […] **ermutigt** werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte […] zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen…“*

Der „schwarze Peter“ bleibt aber bei dem Verantwortlichen, sofern er sich für das „falsche Produkt“ entscheidet und somit gegen diese Grundsätze verstößt (und dafür haften muss).

Insgesamt werden Unternehmer von allen Seiten immer mehr in den Bereich von nicht-datenschutzkonformer „Cloud“-Software gedrängt (siehe Seite 650 und 662). Denken wir beispielsweise an WhatsApp, oder an Microsoft® mit seinen immer stärker an der Cloud angebundenen Softwareprodukte (siehe Seite 186 und 652). [32]

[32] Insbesondere mit „Microsoft 365“ wird ein Unternehmen schnell „in die Cloud“ gezogen. Mittels hoher Preise (und nur kurzen Service-Intervallen) wird eine rein lokal installierte Office-Installation zusehends uninteressant. Ehe man sich versieht hat man sämtliche Server-Funktionalitäten auf die Server von Microsoft ausgelagert. Bisher steht Microsoft nicht in dem Verdacht, dass man dort die Grundsätze von Datenminimierung und datenschutzfreundlicher Technikgestaltung besonders beachten würde.

[Ab hier eine Lücke aufgrund der Leseprobe...]

3.3 Verarbeitungsverzeichnis des Verantwortlichen [GVO_030]

Dokumentation und Nachweis

Die Dokumentation der Verarbeitungstätigkeiten gemäß Artikel 30 durch den Verantwortlichen ist besonders wichtig. Jede einzelne Verarbeitung muss präzise dokumentiert werden. Ohne eine solche Dokumentation kann das Unternehmen nicht garantieren, dass der Umgang mit personenbezogenen Daten datenschutzrechtlich zulässig ist.

Dieser Pflicht wird das Kürzel **[GVO_030]** zugeordnet (siehe Seite 14).

3.3.1 Allgemeine Informationen zur Pflicht [GVO_030]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Neue Literatur im Mai: Die GDD-Praxishilfe DS-GVO V wurde aktualisiert (aber nur die Version für den Verantwortlichen) und MS-Word-Vorlagen finden sich hier ● Die GDD hat den VVZ-Praxisleitfaden im März 2020 überarbeitet. ● Die Aufsichtsbehörden liefern beispielhafte Verarbeitungs-Dokumentationen. ● Das DSK-Kurzpapier-1 im Juli 2017 ● Sehr gute Erläuterungen finden sich in der Trainingseinheit 2 („Dokumentationspflichten“) der Informationsreihe „Fit für die Datenschutz-Grundverordnung“. ● Das Buch „Verfahrensverzeichnis 2.0“ von Markus Schäffter beschreibt alles detailliert ab Seite 32.

[Im Rahmen des PrivazyPlan® wird das Dossier „Verzeichnis von Verarbeitungstätigkeiten“ 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.]

3.3.2 Was bedeutet diese Pflicht [GVO_030] ?

Das Verarbeitungsverzeichnis soll einen Überblick darüber verschaffen, welche personenbezogenen Daten der Verantwortliche auf welche Weise verarbeitet.

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 612 ausführlich erläutert.

\PrivazyPlan\GVO_030
… dort finden Sie beispielhafte Dokumente zum Verarbeitungsverzeichnis. (Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

a) Was ist eine Verarbeitung?

Was ist eine **Verarbeitung aus theoretischer Sicht**? Der Artikel 4 Nr. 2 besagt: Die *Verarbeitung* führt eine Reihe von Vorgängen auf Daten aus, und nutzt hier für automatisierte Verfahren (oder nicht-automatisierte Verfahren, siehe Seite 613). Diese Definition hilft wohl niemandem weiter. Wie schon im BDSG-alt, so erklärt auch die DS-GVO hierzu keine weiteren Details.

Der Kommentar von Kühling/Buchner erörtert die Sachverhalte sehr ausführlich in RdNr. 11-39 zu Artikel 4 Nr. 2.

Rein **praktisch gesehen** ist eine Verarbeitung beispielsweise Folgendes:

- Führen der Personalakte
- Lohn- und Gehaltsabrechnung
- Betreiben einer Internet-Website (inkl. z.B. der Nutzungsauswertung per Google Analytics)
- Newsletter-Versand
- Videoüberwachung (siehe „weiche“ Pflicht **[AUX_012]** auf Seite 622)
- Kundenbetreuungs-Software (CRM)
- Lieferantendokumentation
- E-Mail Server betreiben
- und vieles mehr…

Es ist nicht trivial, die große Menge der Datenverarbeitungen in solch ein Denkschema zu überführen. Die deutschen Aufsichtsbehörden haben es in 40 Jahren nicht geschafft, hierzu eine konkrete und praxistaugliche Anleitung zu liefern.

Im Datenschutz-Berater 04/2019 auf Seite 82-83 wird auf die Schwierigkeit der konkreten Eingrenzung von Verarbeitungen eingegangen.

➔ Bitte berücksichtigen Sie bei der „Identifikation der Verarbeitungen“ unbedingt die „Strukturanalyse hinsichtlich der Geschäftsprozesse“ auf Seite 409.

[Ab hier eine Lücke aufgrund der Leseprobe...]

3.4 Verarbeitungsverzeichnis des Auftragsverarbeiters [GVO_030a]

Dokumentation und Nachweis

Im Rahmen von Outsourcing hat jeder Auftragsverarbeiter gemäß Artikel 30 (2) seine Dienstleistungen zu dokumentieren. Dies umfasst auch die Namen und Kontaktdaten seiner Auftraggeber. Somit hat der Auftragsverarbeiter stets eine genaue Übersicht darüber, welche Leistungen er für welche Kunden erbringt.

Dieser Pflicht wird das Kürzel **[GVO_030a]** zugeordnet (siehe Seite 14).

3.4.1 Allgemeine Informationen zur Pflicht [GVO_030a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

ACHTUNG: In der deutschen Übersetzung des Artikel 30 (5) hat sich ein schwerer Übersetzungsfehler eingeschlichen, der den Sinn komplett entstellt (siehe Seite 518).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● „Heidelberger Kommentar“ zum Artikel 30 (2) auf Seite 689-693… aus unserer Sicht der einzige Kommentar, der sich wirklich konkret und lesenswert äußert ● Die Aufsichtsbehörden liefern beispielhafte Verarbeitungs-Dokumentationen. ● Die GDD-Praxishilfe DS-GVO V geht etwas detaillierter auf diese Pflicht ein.

3.4.2 Was bedeutet diese Pflicht [GVO_030a] ?

a) Wo liegt der Sinn?

Warum muss der Auftragnehmer eine solche Dokumentation erstellen? Die Fachkommentare äußern sich dazu leider nicht. Denkbar wären die folgenden Überlegungen:

Sollte der Auftragnehmer feststellen, dass bei ihm eine „*Verletzung des Schutzes personenbezogener Daten*“ stattgefunden hat (im Sinne des Artikel 4 Nr. 12), dann besteht akuter Handlungsbedarf. Es ist sicherzustellen, dass die verantwortlichen Auftraggeber innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde bzw. unverzüglich an die betroffenen Personen machen können (siehe Artikel 33 bzw. Artikel 34). Dies ist nur dann sicher gewährleistet, wenn der Auftragsverarbeiter sofort und zuverlässig die betroffenen Verantwortlichen herausfinden und informieren kann.

Der Zeitdruck steigt schlagartig an, wenn es eine Kette von Auftragsverarbeitern gibt, und die Datenschutzverletzung z.B. beim fünften Unter-Auftragsverarbeiter begangen wurde. Insofern macht diese von Brüssel geforderte Liste absolut Sinn.

Was würde denn passieren, wenn der Auftragnehmer seine Auftraggeber nicht schnellstmöglich über eine Datenschutzverletzung informieren würde? Der verantwortliche Auftraggeber hätte ein Problem, denn er könnte **(a)** seinen Meldungspflichten nicht nachkommen und müsste mit Geldbußen und Schadenersatzforderungen rechnen (siehe ab Seite 575) und könnte **(b)** keine schnellen Gegenmaßnahmen einleiten, um den Schaden zu minimieren.

Und wer muss wohl letztlich für diese Schäden aufkommen? Vermutlich der Auftragnehmer! Insofern sollte jeder Auftragnehmer ein vitales Interesse daran haben, dass er die hier im Artikel 30 (2) geforderte Dokumentation gewissenhaft erfüllt.

b) Was muss dokumentiert werden?

Auf den ersten Blick scheint es, dass sich die Absätze 1 und 2 des Artikel 30 stark ähneln. Doch das täuscht. Der Absatz 1 erlegt dem Verantwortlichen weitgehend andere Dokumentationspflichten auf, als dem Auftragsverarbeiter in Absatz 2. Die folgenden Aspekte sind wichtig:

- **Schritt 1:** Nennung **der verantwortlichen Auftraggeber**
  Gemäß Artikel 30 (2a) muss eine Liste aller Auftraggeber erstellt werden. Zu nennen sind die Kontaktdaten, wie Firmenname, Ansprechpartner, Postadresse, Telefon und E-Mail. Außerdem muss der jeweilige Datenschutzbeauftragte mit seinen Kontaktdaten genannt werden.

  Doch wie ist dies zu verstehen, wenn die Datenverarbeitung aus einer ganzen Kette von Auftragsverarbeitern besteht? Ziemlich wahrscheinlich wird wohl jeder Auftragsverarbeiter nur „seinen eigenen Auftraggeber“ als Verantwortlichen nennen müssen.

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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.

- Das **berechtigte Interesse** des Verantwortlichen ist sorgsam abzuwägen. Er muss eine Interessenabwägung nachweisen können (siehe Seite 338). 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.

Hinzukommen aber noch andere Aspekte der Rechtmäßigkeit. Insbesondere bei dem Daten-Transfer an Dritte (innerhalb und außerhalb der EU/EWR) wird diese Frage nochmal aufkommen (siehe Pflicht **[GVO_044]** auf Seite 222).

4.1 Datenverarbeitungen brauchen eine Rechtsgrundlage [GVO_006]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 6 darf der Verantwortliche personenbezogenen Daten nur dann 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 bieten hier ca. 30 Möglichkeiten. Bei sensiblen Daten gelten besonders hohe Hürden.

Dieser Pflicht wird das Kürzel **[GVO_006]** zugeordnet (siehe Seite 14).

4.1.1 Allgemeine Informationen zur Pflicht [GVO_006]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Die Datenschutz-PRAXIS 12/2019 berichtet auf Seite 5-7 über das konkrete Auffinden der Rechtsgrundlage ● Der Verkauf von Kundendaten („Asset Deal“, Schuldübernahme gemäß § 414f BGB) wird in einem DSK-Beschluss thematisiert; hier sind die Begriffe „Genehmigung“ und „Zustimmung“ möglicherweise im Sinne einer „Einwilligung“ zu verstehen. Siehe auch hier und hier. ● **VdS-Richtlinie 10010** (Seite 512) im dortigen Kapitel 10.7 („Rechtsgrundlage“).

[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. [36]

Was ist überhaupt eine „Verarbeitung“? Auf den ersten Blick auf Artikel 4 Nr. 2 wirkt die Frage trivial. Doch es gibt so einige Grenzfälle, wie z.B. „aufgedrängte Daten“, die die Verantwortlichen nicht erheben wollten (wie z.B. Initiativbewerbungen). Oder Archivbestände von Patientenakten, die einem Unternehmen im Rahmen von Insolvenz sozusagen in den Schoß fielen. Oder Attrappen von Videokameras. Die DuD 09/2021 beschäftigt sich auf Seite 603-608 intensiv mit dieser Frage. Hier werden auch die Szenarien „Server-Housing“ und „Lagerhaltung“ thematisiert. Kurz gesagt: es muss „willensgetragenes menschliches Handeln“ zugrunde liegen, welches eine „Veränderung des Zustands der Daten“ bewirkt.

In Deutschland droht der § 42 BDSG mit einer **Freiheitsstrafe** von bis zu 3 Jahren, wenn personenbezogene Daten unberechtigt verarbeitet werden (und dies zur eigenen Bereicherung oder mit schädigen Absichten geschieht).

[36] Erstaunlicherweise verhängte die griechische Datenschutz-Aufsichtsbehörde eine Geldbuße von 150.000 €, weil ein Unternehmen sich für eine **falsche Rechtsgrundlage** entschieden hatte (siehe http://www.enforcementtracker.com/ am 30.07.2019). Hier wird berichtet, dass das Unternehmen irrtümlicherweise eine Einwilligung nutzte, obwohl die Verarbeitung zum Zwecke des Arbeitsvertrags erforderlich war. Die Geldbuße ist reichlich hoch für diesen verhältnismäßig trivialen Rechtsirrtum.

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.2 Zweckänderungen müssen sorgsam geprüft werden [GVO_006a]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 6 (4) sind Zweckänderungen nur unter sehr engen Voraussetzungen erlaubt. Genau genommen kann man nur von „Zweck-Erweiterungen“ sprechen. Gibt es hierfür keine Einwilligung und kein Gesetz als Rechtsgrundlage, so hat der Verantwortliche eine ausführliche Abwägung durchzuführen.

Dieser Pflicht wird das Kürzel **[GVO_006a]** zugeordnet (siehe Seite 14).

4.2.1 Allgemeine Informationen zur Pflicht [GVO_006a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

⚠ Der Erwägungsgrund 50 thematisiert die Zweckänderung sehr ausführlich. Für ein Verständnis dieses Themas ist dieser Erwägungsgrund unverzichtbar.

Im Bundesdatenschutzgesetz erlaubt der § 24 Abs. 1 BDSG u.a. eine Übermittlung an die Polizei zwecks Verfolgung von Straftaten (siehe Seite 535).

Siehe auch die Pflicht **[GVO_013a]** zur Mitteilung von Zweckänderungen auf Seite 137.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente. ● Sehr tiefgehende Analyse der Problematik hier ● Die RDV 03/2018 berichtet auf Seite 145-153 speziell zu Beschäftigtendaten. ● Die Zeitschrift ZD 11/2016 berichtet auf Seite 507-512.

[Im Rahmen des PrivazyPlan® wird das Dossier „Zweckbindung“ und das Dossier „Zweckänderung“ 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.]

4.2.2 Was bedeutet diese Pflicht [GVO_006a] ?

Speziell hier in Bezug auf die Zweckänderung ist die Gefahr von Geldbußen besonders tückisch: Eine unbewusste Zweckänderung ist schnell passiert und hat enorme Auswirkungen! Ein stark motivierter Vertriebsmitarbeiter kommt ständig auf neue Ideen, wie er personenbezogene Daten für werbliche Zwecke nutzen kann; die Notwendigkeit zur Konformität mit bisher fest definierten Zwecken wird da schnell übersehen. Diese Datenverarbeitungen sind dann illegal und können schwerwiegende Konsequenzen nach sich ziehen.

a) Zunächst gilt das Prinzip der „Zweckbindung“

Die zunächst geltende Zweckbindung einer Verarbeitung leitet sich aus Artikel 5 (1b) ab. Im Rahmen von Einwilligungen wird vorausgesetzt, dass diese für „bestimmte“ Zwecke gegeben wurden; siehe Artikel 6 (1a) und Artikel 9 (2a). Überprüfbar ist die Zweckbindung seitens der betroffenen Personen insbesondere durch die Informationspflichten gemäß Artikel 13 (1c) und Artikel 14 (1c). Das Unternehmen dokumentiert die genauen Zwecke einer Verarbeitung im Verarbeitungsverzeichnis gemäß Artikel 30 (1b), was durch die Aufsichtsbehörde kontrollierbar ist.

Schon diese skizzenhafte Darstellung beweist die Wichtigkeit der Zweckbindung recht deutlich. Eine Zweckänderung kann durch betroffene Personen und Aufsichtsbehörden leicht festgestellt werden; das kann teuer werden.

b) Die Fachwelt streitet über den Begriff der „Vereinbarkeit“

Der Artikel 6 (4) eröffnet die Möglichkeit einer „Verarbeitung zu einem anderen Zweck“, sofern dieser „**vereinbar**“ mit dem ursprünglichen Zweck ist.
Die Fachliteratur ist sich aber bei der Interpretation des Begriffes „vereinbar“ (engl. „compatible“) völlig uneinig. Manche Autoren behaupten, dass der Satz 2 im Erwägungsgrund 50 ein redaktioneller Fehler sei, andere Autoren bestreiten das vehement.
Es ist schon erstaunlich, dass die Fachwelt bei so einer zentral wichtigen Frage keinen Konsens findet. Andererseits: Je öfter man sich den Artikel 6 (4) durchliest, desto mehr fragt man sich, warum Brüssel nicht einfach klar und unverblümt formuliert, wie genau die Rechte und Freiheiten der betroffenen Personen zu schützen seien. Jedenfalls liefert die Fachliteratur zwar viele Worte, aber wenig pragmatischen Inhalt.

Das Verständnis des Begriffs „Vereinbarkeit“ wird auch nicht unbedingt erleichtert, wenn man im Erwägungsgrund 50 liest: „*Die Weiterverarbeitung für im öf-*

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.3 Einwilligungen müssen dauerhaft nachweisbar sein [GVO_007]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 7 (1) muss das Unternehmen die Einwilligungen der betroffenen Personen nachweisen können. Es bedarf also einer ausführlichen Dokumentation darüber WER seine Einwilligung WANN und WIE gegeben hat und welcher WORTLAUT genau vorlag. Vermutlich macht es Sinn, dass man eventuelle Widerrufe in genau der gleichen Form dokumentiert.

Dieser Pflicht wird das Kürzel **[GVO_007]** zugeordnet (siehe Seite 14).

4.3.1 Allgemeine Informationen zur Pflicht [GVO_007]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● DSK-Kurzpapier-20 fasst das Thema „Einwilligung" gut zusammen ● Die Artikel-29-Datenschutzgruppe hat das Workingpaper „WP 259" veröffentlicht, wo auf 31 Seiten in Englisch viele Aspekte erläutert werden [51]. ● Die GDD-Praxishilfe DS-GVO XIII geht auf Einwilligungen ein. ● Die Datenschutz-PRAXIS berichtet in der Ausgabe 09/2017 über automatisierte Einwilligungsnachweise („CIAM").

[Im Rahmen des PrivazyPlan® wird das Dossier „Einwilligung" 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.]

[51] Das „WP 259" legt die DS-GVO sehr streng aus und erlegt viele Pflichten und Regeln auf. Die Einwilligung wird dadurch in vieler Hinsicht komplizierter. Hier im PrivazyPlan® kann unmöglich auf alle Aspekte eingegangen werden. Insbesondere in der Einwilligungs-Checkliste hat Nicholas Vollmer versucht die wichtigsten Aspekte zu berücksichtigen (siehe Seite 298).

4.3.2 Was bedeutet diese Pflicht [GVO_007] ?

a) Große Bedeutung im Datenschutzrecht

Der Einwilligungs-Nachweis hat eine große Bedeutung im Datenschutzrecht. Erfahrungsgemäß resultieren viele Konflikte (mit Betroffenen und Aufsichtsbehörden) daraus, dass die betroffene Person behauptet keine Einwilligung gegeben zu haben. In den klassischen Fällen (z.B. bei Newsletter-Anmeldung) lässt sich dies meist einfach widerlegen, sofern man die Anmeldungen gewissenhaft protokollierte.

Der Verantwortliche hat wohl ein großes Interesse daran, dass solche Konflikte nicht eskalieren. Daher sollte er zwei Dinge sicherstellen:

- Dass die fraglichen Einwilligungen schnell und sicher nachgewiesen werden können. Dies ist das Anliegen der hier vorliegenden Pflicht **[GVO_007]**.
- Eine präzise Dokumentation der jeweiligen Einwilligung ist auch wichtig für deren Widerrufsmöglichkeit. Der Widerruf darf gemäß der Pflicht **[GVO_007b]** auf Seite 148 nicht komplizierter sein als die Einwilligung selbst. Doch dafür muss man in jedem Einzelfall wissen, wie einfach/schwierig die jeweilige Einwilligung ursprünglich war.
- Dass sich die betroffenen Personen nicht zuerst an die Aufsichtsbehörde wenden, sondern direkt an den Verantwortlichen bzw. dessen Datenschutzbeauftragten wenden. Dies stellt die Pflicht **[GVO_038b]** auf Seite 250 sicher. Auch die Auskunftspflichten **[GVO_013]** auf Seite 39 und **[GVO_014]** auf Seite 50 können zu diesem Zweck genutzt werden.

Je höher die Beweiskraft dieser Nachweise ist, desto unwahrscheinlicher eskaliert die Beschwerde einer betroffenen Person. Beim Nachweis sollte also vielleicht nicht der Grundgedanke der Datenminimierung gelten, sondern eher die Präzision.

Insbesondere die **Einwilligung zur Telefonwerbung** ist nicht einfach nachzuweisen (siehe Datenschutz-Berater 05/2019 auf Seite 107, der das BGH-Urteil I ZR 164/09 vom 10.02.2011 erwähnt und auf zwei Aufsichtsbehörden-Stellungnahmen eingeht: hier auf Seite 103 und hier auf Seite 113).

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.4 Einwilligungstexte müssen klar erkennbar und gut verständlich sein [GVO_007a]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 7 (2) dürfen Einwilligungstexte nicht versteckt oder verklausuliert werden. Wird dies nicht berücksichtigt (oder sollten sie auch sonst gegen die Verordnung verstoßen), so sind die betroffenen Teile der Einwilligung unwirksam (und jene Teile der Verarbeitung unrechtmäßig).

Dieser Pflicht wird das Kürzel **[GVO_007a]** zugeordnet (siehe Seite 14).

4.4.1 Allgemeine Informationen zur Pflicht [GVO_007a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Die Artikel-29-Datenschutzgruppe hat das Workingpaper „WP 259“ veröffentlicht (siehe die Fachliteratur-Anmerkungen im Kapitel 4.3 auf Seite 142).

[Im Rahmen des PrivazyPlan® wird das Dossier „Einwilligung“ 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.]

4.4.2 Was bedeutet diese Pflicht [GVO_007a] ?

Die „verständliche und leicht zugängliche Form“ ist wichtig. Demnach dürfen Einwilligungen nicht durch unverständliche Mechanismen erschlichen werden. Sie dürfen auch nicht irgendwo in anderen Texten versteckt werden. Da aber die DS-GVO sowieso kein Opt-Out mehr zulässt, ist diese Vorgabe zukünftig wohl nicht mehr sehr relevant (weil keine voraus angekreuzten Kästchen versteckt werden können). Andererseits dürfen gemäß dem Gola-Fachkommentar in RdNr. 41-43 zu Artikel 7 die Einwilligungen auch in AGBs enthalten sein; insofern ist die Hervorhebung sehr wichtig.

Die Forderung nach einer klaren und einfachen Sprache ist sehr wichtig. Die Gerichte stellen insbesondere bei Werbe-Einwilligungen stets sehr hohe Anforderungen an die Klarheit und Präzision von Einwilligungstexten. Jegliche Mehrdeutigkeit oder Unschärfe gilt es zu vermeiden. Jeder „Fehler“ kann von spitzfindigen Juristen als eine Übervorteilung angesehen werden.

4.4.3 Wie erfüllt man diese Pflicht [GVO_007a] ?

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: ● Einwilligungstexte müssen klar erkennbar sein. ● Einwilligungstexte müssen präzise und verständlich sein ● ➔ Nutzen Sie das Beispielformular von Seite 350.

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 24.

b) Durchführung („do“)

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

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 25.

Es bedarf vorbereitender Maßnahmen, bevor diese Pflicht durchgeführt werden kann:

☐ Wollen Sie das ➔ Beispielformular von Seite 350 nutzen? Dort finden Sie alle konkreten Schritte zur Planung und Formulierung von Einwilligungen. Dann passen Sie es zunächst auf Ihre Belange an.

Im konkreten Fall ist folgendes zu tun:

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.5 Einwilligung muss jederzeit (und einfach) widerrufbar sein [GVO_007b]

Gemäß Artikel 7 (3) muss eine Einwilligung jederzeit widerrufbar sein. Hierüber ist die Person vorab zu informieren. Der Widerrufsvorgang darf nicht komplizierter sein als der zugrundeliegende Einwilligungsvorgang.

Dieser Pflicht wird das Kürzel **[GVO_007b]** zugeordnet (siehe Seite 14).

4.5.1 Allgemeine Informationen zur Pflicht [GVO_007b]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Die Artikel-29-Datenschutzgruppe hat das Workingpaper „WP 259“ veröffentlicht (siehe die Fachliteratur-Anmerkungen im Kapitel 4.3 auf Seite 142).

[Im Rahmen des PrivazyPlan® wird das Dossier „Einwilligung“ und das Dossier „Widerruf“ 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.]

4.5.2 Was bedeutet diese Pflicht [GVO_007b]?

Generell gilt wie schon zu alten BDSG-Zeiten, dass eine Einwilligung jederzeit widerrufbar ist. Genau dies macht diesen Erlaubnistatbestand oftmals so schwierig, denn meist lassen sich darauf keine umfassenden Geschäftsmodelle oder -prozesse aufbauen. Es reicht ja immer eine einzige Person, die aus irgendwelchen Gründen ihre Einwilligung zurückzieht.

Übrigens muss man das hier thematisierte Widerrufsrecht unterscheiden vom „Widerspruch gegen eine Verarbeitung“ im Sinne des Artikel 21 und der Pflicht **[GVO_021]** auf Seite 93. Es ist denkbar, dass eine betroffene Person diese Begriffe verwechselt.

a) Widerruf muss jederzeit möglich sein

Damit ein Widerruf jederzeit möglich ist, müssen die betroffenen Personen zunächst Kenntnis von dieser Widerrufsmöglichkeit haben. Diese Transparenz ist insofern gegeben, als dass die betroffenen Personen bereits durch frühzeitige Informationen durch die Pflichten **[GVO_013]** und **[GVO_014]** über das Widerrufsrecht unterrichtet wurden (siehe Seite 39 und Seite 50). Sicherheitshalber sollte auch der eigentliche Einwilligungstext das Widerrufsrecht erwähnen (siehe auch hier).
(Eventuell wird auch auf freiwilliger Basis im Rahmen der allgemeinen Auskunftspflicht **[GVO_015]** auf die eventuelle Widerrufsmöglichkeit hingewiesen; siehe Seite 55.)

Die widerrufende Person muss sicher **identifiziert** werden, bevor der Widerruf gespeichert wird. Es ist ja nicht auszuschließen, dass eine fremde Person betrügerisch eine Einwilligung widerruft. Beispielsweise im Falle von Telefon- und Postkarten-Einwilligungen ist diese Identifikation nicht trivial, denn die betroffene Person darf dann auch per Telefon oder Postkarte widerrufen.

[Im Rahmen des PrivazyPlan® wird das Dossier „Identifizierung“ 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.]

b) Widerruf muss einfach möglich sein

Sehr interessant ist die Forderung, dass der Widerruf nicht komplizierter als die Einwilligung sein darf. Dies macht Sinn, denn es gab rücksichtslose Unternehmen, denen genügte eine telefonische Einwilligung, jedoch zum Widerruf forderten sie ein Einschreiben mit Rückschein, um die betroffenen Personen abzuschrecken.

Dieses Ungleichgewicht ist aus der Welt. Dies ist für die betroffenen Personen sehr angenehm. Doch für den Verantwortlichen bedeutet dies, dass er jederzeit genau wissen (und nachweisen!) können muss, auf welchem Weg die Einwilligung erteilt wurde. Dies wird durch die Pflicht **[GVO_007]** auf Seite 142 sichergestellt (sofern man im Rahmen der Dokumentationspflicht auch daran denkt, den jeweiligen Einwilligungsweg zu dokumentieren).

c) Was passiert nach einem Widerruf?

Wenn der Widerruf erfolgt, so sollte dieser genau dort dokumentiert werden, wo auch die dazugehörige Einwilligung dauerhaft dokumentiert war (siehe Pflicht **[GVO_007]** auf Seite 142). Würde man anders vorgehen (und die Einwilligungen

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.6 Die Freiwilligkeit von Einwilligungen muss unbestreitbar sein [GVO_007c]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 7 (4) müssen Einwilligungen wirklich freiwillig sein. Dies betrifft zahlreiche sehr verschiedene Aspekte: Wirksame Einwilligungen sind frei von Zwang und werden in voller Kenntnis aller Umstände (inkl. Widerrufsrecht) erteilt. Der Verantwortliche sollte die weitere Vertragserfüllung möglichst nicht von (vertraglich nicht-erforderlichen) Einwilligungen abhängig machen.

Dieser Pflicht wird das Kürzel **[GVO_007c]** zugeordnet (siehe Seite 14).

4.6.1 Allgemeine Informationen zur Pflicht [GVO_007c]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5a) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Die Artikel-29-Datenschutzgruppe hat das Workingpaper "WP 259" veröffentlicht (siehe die Fachliteratur-Anmerkungen im Kapitel 4.3 auf Seite 142). ● Die „Zeitschrift für Datenschutz" berichtet ausführlich in der Ausgabe 02/2018 Seite 55-62.

[Im Rahmen des PrivazyPlan® wird das Dossier „Einwilligung" 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.]

4.6.2 Was bedeutet diese Pflicht [GVO_007c] ?

Der Artikel 7 (4) thematisiert eigentlich nur die unbefugte Kopplung von Vertragserfüllung und Einwilligung. Doch im Detail ist das wohl nicht so leicht zu interpretieren.

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 (siehe Seite 590).

a) Kopplungsverbot (Vertrag nicht abhängig machen von irrelevanten Einwilligungen)

Dieses Kriterium ist direkt dem Artikel 7 (4) zu entnehmen. Der Verantwortliche sollte einen Vertrag oder eine Dienstleistung möglichst nicht von einer Einwilligung abhängig machen, die inhaltlich nichts mit dieser Leistung zu tun hat.

Der Wortlaut dieses Artikel 7 (4) ist zu verschachtelt, als dass der normale Leser ihn verstehen könnte (in der obigen Webseite haben wir versucht den Satz durch Hervorhebungen besser lesbar zu gestalten).

Einen guten Interpretationsansatz liefert der Paal/Paul-Fachkommentar in RdNr 20 zu Artikel 7: Die **Erfüllung eines (bestehenden) Vertrages** darf der Verantwortliche nicht davon abhängig machen, dass die betroffene Person ihre Einwilligung für solche Verarbeitungen erteilt, die für die eigentliche Vertragserfüllung nicht notwendig sind. [53]
Demnach wäre eine Formulierung der folgenden Art unzulässig: „*Sehr geehrter Kunde, um unseren Gas-Lieferungs-Vertrag weiterhin erfüllen zu können ist die folgende Einwilligung notwendig: ☐ Ja, ich willige ein, dass meine E-Mail-Adresse zu Werbezwecken meines Energieversorgers genutzt werden darf.*"

Es ist die Frage, wann die kritische Schwelle einer „Einwilligungs-Nötigung" erreicht ist. Die Beurteilung ist trivial, wenn eine verweigerte Einwilligung (in eine nicht-erforderliche Verarbeitung) zu einer faktischen Leistungsverweigerung des Verantwortlichen führen würde.

In vielen anderen Fällen wird es legitim sein, dass der Verantwortliche seine Leistungen (zugunsten des Kunden) erweitern möchte und hierfür eine Einwilligung einholt.
Beispiel: Ein Verantwortlicher richtet eine Kantine ein, wo die Beschäftigten freiwillig zu Mittag essen können. Die Bezahlung soll über die Gehaltsabrechnung erfolgen. Es bedarf einer Einwilligung, dass die notwendigen Daten (Personalnummer, Verzehrdaten) hierfür genutzt werden dürfen, weil der normale Arbeits-

[53] Sofern Paal/Pauly dies wirklich auf Erfüllung bestehender (!) Verträge beziehen, so ist die Interpretation sehr sinnvoll. Es ist in der Tat moralisch grenzwertig, wenn man bestehende Verträge missbraucht, um sich **nicht-erforderliche** Datenverarbeitung per „Einwilligung" legitimieren zu lassen. Das wäre das „Friss-oder-Stirb"-Prinzip in Reinform.

[Ab hier eine Lücke aufgrund der Leseprobe...]

4.7 Einwilligungen von Kindern durch Eltern legitimieren [GVO_008]

Rechtmäßigkeit und Einwilligung

Gemäß Artikel 8 (2) gibt es eine Besonderheit bei der Einwilligung durch Kinder. Sofern sich Dienste der Informationsgesellschaft explizit an Kinder unter 16 Jahren richten, so müssen „angemessene Anstrengungen“ unternommen werden, um die Zustimmung der Eltern - gemäß Artikel 8 (1) - einzuholen. Andernfalls kann die Einwilligung unrechtmäßig sein.

Dieser Pflicht wird das Kürzel **[GVO_008]** zugeordnet (siehe Seite 14).

4.7.1 Allgemeine Informationen zur Pflicht [GVO_008]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Hier wird ausführlich über die (Daten-) Verarbeitung von Kindern berichtet. ● In der RDV 09/2021 auf Seite 505-508 wird berichtet. ● Die PinG 05/2020 berichtet auf Seite 208-214 über Kinder und Datenschutz.

[Im Rahmen des PrivazyPlan® wird das Dossier „Einwilligung“ und das Dossier „Identifizierung“ 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.]

4.7.2 Was bedeutet diese Pflicht [GVO_008] ?

Wenn die Betreiber von Webseiten und Internetspielen die Daten von minderjährigen erheben und speichern wollen, so sollen sie die Zustimmung der Eltern einholen.

Der Träger der elterlichen Verantwortung soll also entweder die Einwilligung erteilen oder seine Zustimmung zum Einverständnis des Kindes geben.

Praktisch gesehen stellt diese Pflicht den Verantwortlichen vor eine schwierige Herausforderung: Wie soll man wissen **(a)** ob wirklich ein Kind betroffen ist, und **(b)** ob die erwachsene Person tatsächlich die elterliche Verantwortung trägt und **(c)** ob das Kind nicht selbst vorgibt diese elterliche Person zu sein?

Gemäß vieler Fachkommentare gilt der folgende Weg als gangbar: **(a)** Für die Feststellung, ob es sich um ein Kind handelt, reicht es aus, dass man in einer Eingabemaske das Alter ausdrücklich und kindgerecht abfragt. **(b)** Der Träger der elterlichen Verantwortung wird ermittelt, indem das Kind die E-Mail-Adresse dieser Person nennt. **(c)** Diese elterliche E-Mail-Adresse enthält einen Hyperlink, dessen Anklicken dann die Einwilligung (mit Zustimmung) ausdrückt.

Selbstverständlich ist diese Vorgehensweise in keiner Form sicher, aber dies scheint derzeit der Stand der Technik zu sein. Alternativ wäre denkbar:

- ein von den Eltern unterschriebenes Dokument (per Post oder Scan per E-Mail)
- die Eingabe und Prüfung von Kreditkartendaten
- die Nutzung eines elektronischen Personalausweises der Eltern
- ein Telefongespräch mit den Eltern (alternativ vielleicht auch die Nutzung von Video-Messengern).

Übrigens: Die Eingabe der elterlichen E-Mail-Adresse ist eine „Erhebung bei Dritten“ und löst die Pflicht **[GVO_014]** aus, wie auf Seite 50 beschrieben. Der Elternteil muss also sofort über den Zweck dieser Datenverarbeitung informiert werden.

ACHTUNG: Es besteht eine Öffnungsklausel für die Altersgrenze der Kinder. Die EU-Staaten können diese Grenze auf bis zu 13 Jahre reduzieren. Dies muss berücksichtigt werden, wenn EU-weit die Einwilligungen von Kindern eingeholt werden.

Gemäß Erwägungsgrund 38 gilt diese Pflicht nicht bei Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden. Dadurch soll möglicherweise eine gewisse Diskretion sichergestellt werden.

Auf die lange Sicht ist eine Einwilligung der Eltern nicht unproblematisch, denn irgendwann ist das Kind volljährig und will dann eventuell selbst entscheiden. So sollte z.B. eine Zeitung auch dann um die Einwilligung zur Foto-Veröffentlichung bitten, wenn der Vater diese vor 20 Jahren stellvertretend erteilt hatte (LG Frankfurt, Az. 2-03 O 454/18 vom 29.08.2019).

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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. Eine diesbezügliche Nachweis-, Überwachungs- und Aktualisierungspflicht fordert der Artikel 24 (1). 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 14).

5.1.1 Allgemeine Informationen zur Pflicht [GVO_032]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der neuen Fassung ab dem 25.05.2018) werden durch § 22 Abs. 2 Satz 2 BDSG 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 282 und 283).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Eine 5-seitige Checkliste für den Medizinbereich liefert die Bayerische Aufsichtsbehörde im Mai 2020 ● Siehe VdS-Richtlinie 10000 (siehe Seite 526).

[Im Rahmen des PrivazyPlan® wird das Dossier „Technisch-organisatorische Maßnahmen“ 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.]

5.1.2 Was bedeutet diese Pflicht [GVO_032] ?

Wenn das Unternehmen die Informations-Sicherheit systematisch fördern will, so muss dies gründlich geplant und schnell ausgeführt werden (siehe Seite 524). Diese Pflicht sollte daher möglichst früh bearbeitet werden (eine grobe Priorisierung der Pflichten findet sich auf Seite 19.

Wie wichtig beispielsweise ein Daten-Berechtigungskonzept sein kann, zeigt ein **Bußgeld** von 450.000 € im Oktober 2019 an ein niederländisches Krankenhaus.

Im Dezember 2019 wurde sogar ein **Bußgeld** von 10,4 Mio. Euro gegen 1&1 Telekom wegen mangelhafter technisch-organisatorischer Maßnahmen ausgesprochen (die Identifikation von Anrufern bei einer Telefon-Servicehotline war nicht ausreichend sicher, siehe Seite 566). Auch solche Detail-Aspekte sollten bei der Gestaltung eines ISMS berücksichtigt werden (siehe Seite 524).

Im September 2019 ist tragischerweise wohl das erste Todesopfer eines Hacker-Angriffs zu verzeichnen gewesen: Eine schwer erkrankte Frau konnte vom Notarzt nicht in die naheliegende Düsseldorfer Uniklinik eingeliefert werden, weil die IT dort wegen eine Hackerangriffs ausfiel. Die Staatsanwaltschaft ermittelt wegen fahrlässiger Tötung.

Im Juli 2021 wurde in Deutschland der erste „Cyber-Katastrophenfall“ ausgerufen. Der Landkreis Anhalt-Bitterfeld wurde Opfer eines Cyberangriffs und war wochenlang lahmgelegt.

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 Compu-

[Ab hier eine Lücke aufgrund der Leseprobe...]

5.2 Beschäftigte Personen sind konkret anzuweisen [GVO_032a]

Sicherheit und Datenschutzverletzungen

Der Artikel 32 (4) fordert konkrete (Arbeits-) Anweisungen für die Beschäftigten, damit diese datenschutzkonform arbeiten. Dadurch wird verhindert, dass Mitarbeiter aus Unwissenheit, Desinteresse, Überengagement usw. fehlerhaft arbeiten (indem sie z.B. Beschwerden ignorieren, technische Maßnahmen umgehen, eigenmächtig Daten in der Cloud speichern). Dieser Absatz 4 macht klar, dass die „Sicherheit der Verarbeitung" nicht nur eine technische Herausforderung ist, sondern auch eine menschliche.

Dieser Pflicht wird das Kürzel **[GVO_032a]** zugeordnet (siehe Seite 14).

5.2.1 Allgemeine Informationen zur Pflicht [GVO_032a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der Fassung ab dem 25.05.2018) gibt es eine zusätzliche Sensibilisierungspflicht im Gesundheits- und Sozialbereich. Siehe Pflicht **[BDSG_022]** auf Seite 282.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente ● Die Bayerische Aufsichtsbehörde veröffentlicht ein Musterbeispiel für eine Datenschutz-Verpflichtung.

5.2.2 Was bedeutet diese Pflicht [GVO_032a] ?

Interessant ist der fast gleiche Wortlaut in Artikel 29 (der aber eher darauf abzielt, dass der Verantwortliche auch Weisungen an die Beschäftigten des Auftragsverarbeiters erteilen darf); dies betrifft dann eher die Pflicht **[GVO_028a]** auf Seite 214.

a) Große Unklarheit über Bedeutung dieser Rechtsvorschrift

Die Fachliteratur streift diesen Artikel 32 (4) nur oberflächlich. Die Zeitschrift RDV 04/2016 spricht auf Seite 200 von „*Prozessbeschreibungen und Arbeitsanweisungen*". Der Kommentar von Kühling/Buchner nennt in RdNr. 38 zu Artikel 32 lediglich „*Betriebs- oder Dienstanweisungen*". Der Paal/Pauly-Kommentar sieht in RdNr. 66 zu Artikel 32 „*die Etablierung eindeutiger Verhaltensregeln und Dienstanweisungen*". Der Gola-Kommentar ab RdNr. 47 zu Artikel 32 lässt auch technische Maßnahmen gelten.

Allein der Kommentar von Bergmann/Möhrle/Herb thematisiert diese Pflicht sehr ausführlich in RdNr. 71-84 zu Artikel 32, und formuliert sehr weitgehende Anforderungen. Die wichtigsten Aussagen werden sinngemäß zitiert:

> *„Die Anweisung ist individuell für jeden Mitarbeiter, bezogen auf seinen Arbeitsplatz, zu erstellen. Sie muss folgende Angaben enthalten:*
> - *Rechtsgrundlagen der Verarbeitung;*
> - *Bezeichnung der zulässigen Verarbeitungen;*
> - *Angabe der personenbezogenen Daten, die verarbeitet werden dürfen;*
> - *Hinweis auf das Verbot, personenbezogene Daten unbefugt zu anderen Zwecken zu verarbeiten*
> - *Datensicherungsmaßnahmen, die einzuhalten sind.*
>
> *Die Anweisung ist zum Zeitpunkt der Übertragung der Aufgabe zu erteilen und muss bei einer Änderung des Aufgabengebiets angepasst werden. Die Anweisung ist schriftlich vorzunehmen und dem Mitarbeiter auszuhändigen und in der Personalakte abzulegen. Der Inhalt ist der beschäftigten Person zu erläutern, und es müssen Hinweise gegeben werden, wie sie in der Praxis umzusetzen sind.*
> *Betroffen sind (fast) alle Beschäftigten, auch Aushilfskräfte, Praktikanten, Heimarbeiter, Betriebsrat und Datenschutzbeauftragter. Nicht zum Personenkreis gehören Vorstands- und Aufsichtsratsmitglieder, Unternehmensinhaber, gesetzliche Vertreter von juristischen Personen."*

Diese Entscheidung hat auch große Auswirkung in Bezug auf mögliche Geldbußen. Im Falle eines konkreten Datenschutzverstoßes durch einen Mitarbeiter gibt es zwei Möglichkeiten: **(a)** Der Mitarbeiter hat vorsätzlich einer Anweisung zuwi-

5.3 Datenschutzverletzungen dauerhaft dokumentieren [GVO_033]

Sicherheit und Datenschutzverletzungen

Gemäß Artikel 33 (5) muss der Verantwortliche alle Datenschutzverletzungen sehr detailliert dokumentieren. Das gilt für alle Datenschutzverletzungen gemäß Artikel 4 Nr. 12 (egal, ob geringes, mittleres oder hohes Risiko). Die Aufsichtsbehörde darf diese Dokumentation gemäß Artikel 58 (1a) jederzeit einsehen.

Dieser Pflicht wird das Kürzel **[GVO_033]** zugeordnet (siehe Seite 14).

5.3.1 Allgemeine Informationen zur Pflicht [GVO_033a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es hilfreiche Dokumente: ● 32-seitige EDPB-Guideline 2021-01 zum Thema „Meldepflicht bei Datenschutzverletzung“ mit inoffizieller deutscher Übersetzung ● Basierend auf der (noch nicht endgültigen) EDPB-Empfehlung 01/2021 liefert die Datenschutz-PRAXIS 06/2021 auf Seite 4-5 eine solide Liste zur Vermeidung von Datenschutzverletzungen ● Die GDD liefert im Mai 2021 einen 130-seitigen Ratgeber „Datenpannen“ für 12 € (und als PDF kostenlos für Mitglieder) ● ~~Der 32-seitige Diskussions-Entwurf der EDPB-Guideline 2021-01 zum Thema „Meldepflicht bei Datenschutzverletzung“ mit inoffizieller deutscher Übersetzung, siehe auch~~ Datenschutz-Praxis 05/2021 Seite 5-6. ● Das Workingpaper „WP 250 rev01“ in deutscher Sprache. ● VdS-Richtlinie 10010 (Seite 512) im dortigen Kapitel 13 („Datenschutzvorfälle“) ● Die Artikel-29-Datenschutzgruppe hat am 03.10.2017 das Workingpaper „250“ zur Diskussion gestellt. ● Trainingseinheit 8 der Informationsreihe „Fit für die Datenschutz-Grundverordnung“. ● DatenschutzPraxis 08/2017 Seite 1-4 ● Das Kurzpapier-08 der bayerischen Aufsichtsbehörde.

[Im Rahmen des PrivazyPlan® wird das Dossier „Verletzung des Schutzes“ 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.]

5.3.2 Was bedeutet diese Pflicht [GVO_033]?

a) Was ist eine Datenschutzverletzung?

Die „Verletzung des Schutzes“ wird im Artikel 4 Nr. 12 definiert:

> *„…eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur unbefugten **Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt…“*

Dies betrifft die folgenden Szenarien:

- **Vernichtung von Daten**
  Dies kommt zum Tragen, wenn die Originaldaten unbeabsichtigt/unberechtigt vernichtet werden (nicht betroffen sind Daten-Kopien). Dies könnte beispielsweise durch einen Verschlüsselungs-Trojaner geschehen. Aber auch das versehentliche Vernichten von Akten fällt unter diesen Punkt, ebenso ein Brand- bzw. Wasserschaden an den Original-Personalakten. Dabei ist vorausgesetzt, dass kein Backup existiert.

- **Verlust von Daten**
  Betroffen ist sowohl der materielle Verlust von Datenträgern (z.B. USB-Stick) als auch der Verlust durch Schäden an Festplatten. Dabei ist aber vorausgesetzt, dass es sich um die ORIGINAL-Daten handelt. Denkbar ist das Szenario, dass zentrale IT-Komponenten (Server, Netzwerk-Hardware) durch einen heftigen Blitzeinschlag zerstört wird und tagelang nicht wiederhergestellt werden kann (oder ausgelöst durch Fehlkonfigurationen oder durch Hardware-Diebstahl bzw. -Sabotage). Denkbar ist auch eine Denial-Of-Service-Attacke durch Hacker, die wichtige Websites blockieren und den betroffenen Personen den Zugriff auf deren Daten verhindern.

- **Veränderung von Daten**
  Durch eine Fehlbedienung von Software könnten Daten verändert werden; beispielsweise durch einen fehlerhaften SQL-Befehl, der die Datenbank-

[Ab hier eine Lücke aufgrund der Leseprobe...]

5.4 Datenschutzverletzungen an Aufsichtsbehörde melden [GVO_033a]

Sicherheit und Datenschutzverletzungen

Gemäß Artikel 33 (1) muss eine Datenschutzverletzung innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden, sofern voraussichtlich ein mittleres oder großes Risiko für die „Rechte und Freiheiten“ der betroffenen Personen besteht. Das Unternehmen muss also zunächst eine Risikoprognose erstellen und dann ggf. eine Meldung machen.

Dieser Pflicht wird das Kürzel **[GVO_033a]** zugeordnet (siehe Seite 14).

5.4.1 Allgemeine Informationen zur Pflicht [GVO_033a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit Geldbußen ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 170 und Seite 518) gibt es hilfreiche Dokumente. ● Brüssel arbeitet an einem 32-seitigen Leitfaden zur Meldung von Datenschutzverletzungen; die Entwurfsversion mit vielen praktischen Beispielen findet sich hier. Herr Vollmer kann eine (automatisierte) Übersetzung zur Verfügung stellen. ● In der DuD 02/2020 wird die Frage der Meldepflicht bei Verlust von verschlüsselten Datenträgern ausführlich behandelt. [58] ● Bayern liefert am 01.06.2019 die Version 1.1 einer 64-seitigen Orientierungshilfe „OH-Meldepflichten.pdf“ (siehe auch hier) ● Hamburg veröffentlicht ein 6-seitiges Informationsblatt ● Sehr interessant sind die Ausführungen in der Fachzeitschrift DuD 03/2018 Seite 142-144.

[58] Dort bezieht man sich auf den Grundschutz-Maßnahmenkatalog M 4.337 (hier auf Seite 3917). Die DuD-Autoren sind Juristen und man kann Zweifel haben, ob die technischen Ausführungen wirklich so stimmen. MS-Bitlocker ist natürlich auch OHNE eigenes Passwort auf Basis des TPM wirkungsvoll, denn man kann die Festplatte nicht ausbauen und mit Linux auslesen. Vorausgesetzt ist allerdings, dass alle Computernutzer über ein sicheres MS-Windows-Passwort verfügen (und ein systematisches Ausprobieren verhindert wird). Siehe die EMOTET-Anleitung im Unterverzeichnis \GVO_032\ in der PrivazyPlan.zip – siehe Seite 156).

Das Kernproblem der Fachliteratur besteht darin, dass die Frage der konkreten Risiko-Einschätzung nicht präzise behandelt wird. Der PrivazyPlan® liefert diesbezüglich im Kapitel 12 ab Seite 308 zahlreiche Formulare und Anleitungen.

[Im Rahmen des PrivazyPlan® wird das Dossier „Verletzung des Schutzes“ und das Dossier „Risiko für Rechte und Freiheiten“ und das Dossier „Meldung an Aufsichtsbehörde“ 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.]

5.4.2 Was bedeutet diese Pflicht [GVO_033a] ?

Die Definition von Datenschutzverletzungen findet sich auf Seite 170.

a) Wann besteht eine Meldepflicht an die Aufsichtsbehörde?

Der Verantwortliche hat die Datenschutzverletzung innerhalb von **72 Stunden** zu melden, sofern ein Risiko für die Rechte und Freiheiten der betroffenen Personen abzusehen ist.

Die **72-Stunden-Frist umfasst (mindestens) zwei Arbeitstage**, wie die ZD 04/2019 auf Seite 152-157 ausführlich beschreibt. Die Autoren berufen sich auf die EU-Fristen-Verordnung aus dem Jahr 1971. Gemäß Artikel 3 (5) jener Verordnung „zur Festlegung der Regeln für die Fristen, Daten und Termine“ hat der Verantwortliche immer mindestens ZWEI WERKTAGE Zeit („*Jede Frist von zwei oder mehr Tagen umfasst mindestens zwei Arbeitstage*“). Siehe auch hier.

Manche Aufsichtsbehörden beziehen auch **Wochenenden und Feiertage** ein. Im 28. Saarländischen Tätigkeitsbericht (2019) wird dies auf Seite 58 beschrieben; eine fachliche Begründung wird nicht geliefert und auf andere fachlichen Einschätzungen auch nicht eingegangen. Demnach würde beispielsweise gelten: Wenn die Möglichkeit besteht, dass ein Mitarbeiter an einem Karfreitag von einer Datenschutzverletzung erfährt, dann müsste am Ostermontag ggf. die Meldung erfolgen. Der Verantwortliche müsste demnach also auch an Wochenenden und Feiertagen die personellen Ressourcen sicherstellen. Der Verantwortliche sollte entscheiden, ob er dieser fachlichen Einschätzung folgt.

[Ab hier eine Lücke aufgrund der Leseprobe...]

5.5 Betroffene Person über Datenschutzverletzung benachrichtigen [GVO_034]

Sicherheit und Datenschutzverletzungen

Bei einer Datenschutzverletzung mit voraussichtlich hohem Risiko muss gemäß Artikel 34 (1) die betroffene Person unverzüglich benachrichtigt werden. Eine öffentliche Bekanntmachung kann notwendig sein, wenn die einzelnen Personen nicht erreicht werden können.

Dieser Pflicht wird das Kürzel **[GVO_034]** zugeordnet (siehe Seite 14).

5.5.1 Allgemeine Informationen zur Pflicht [GVO_034]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In Deutschland gibt es weitere Meldepflichten von Datenschutzverstößen z.B. auch im § 109a TKG (siehe Kapitel 3.30 im TOM-Guide®).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

5.5.2 Was bedeutet diese Pflicht [GVO_034] ?

Das Thema „Datenschutzverletzung“ wird ab Seite 174 ausführlich erklärt.

Wie findet man heraus, welche Personen von einer „kompromittierten“ Verarbeitung betroffen sind? Hierüber kann nur das Verarbeitungsverzeichnis Auskunft geben (siehe Seite 110), denn nur hier sind systematisch alle Verarbeitungen aufgeführt.

Leider verwendet die DS-GVO bei dieser sensiblen Pflicht zwei völlig unbestimmte Begriffe, wenn es um die Voraussetzungen der Benachrichtigungspflicht geht. [61]

a) Was bedeutet „voraussichtlich“?

Die Benachrichtigungspflicht besteht nur dann, wenn der Schutz der Rechte und Freiheiten der betroffenen Personen **voraussichtlich** beeinträchtigt wird. Doch was bedeutet „voraussichtlich“ (engl. „is likely to result“)?

Reicht eine Wahrscheinlichkeit von 10% („ist nicht auszuschließen“) oder bedarf es einer Wahrscheinlichkeit von 90% („so gut wie sicher“)? Oder ein Wert dazwischen?

Was bedeutet es, wenn man sagt: „Unsere Ankunft erfolgt voraussichtlich um 19:00 Uhr“? Dahinter steckt doch eine ziemlich sichere bzw. verbindliche Auskunft, die eine hohe Wahrscheinlichkeit ausdrückt. Es wird lediglich ein gewisser Spielraum für unvorhersehbare Ereignisse eingeräumt. Dies entspricht gefühlt einer Wahrscheinlichkeit von mindestens **~75%**.

Im Rahmen der Risikomatrix wird auf Seite 545 auf die verschiedenen Wahrscheinlichkeiten eingegangen. Dort werden die vier Wahrscheinlichkeitskategorien „Vernachlässigbar, begrenzt, wesentlich und maximal“ genannt. Angesichts der obigen Überlegung wäre die Wahrscheinlichkeitskategorie „WESENTLICH WAHRSCHEINLICH“ zutreffend.

b) Was bedeutet „hohes Risiko“?

Die Benachrichtigungspflicht besteht nur dann, wenn dem Schutz der Rechte und Freiheiten der betroffenen Personen ein **hohes Risiko** droht. Doch was bedeutet „hohes Risiko“ (engl. „high risk“)?

Im Verordnungstext finden sich die Ausdrücke „kein Risiko“, „Risiko“, „hohes Risiko“ und „erhebliches Risiko“ (engl. „significant risks“ im Erwägungsgrund 51). Insofern liegt das „hohe Risiko“ gefühlt bei einer Brisanz von **~75%**.

Im Rahmen der Risikomatrix wird auf Seite 546 auf die verschiedenen Wahrscheinlichkeiten eingegangen. Dort werden die vier Wahrscheinlichkeitskategorien „Vernachlässigbar, begrenzt, wesentlich und maximal“ genannt. Angesichts der obigen Überlegung wäre die Wahrscheinlichkeitskategorie „WESENTLICHES RISIKO“ zutreffend.

[Ab hier eine Lücke aufgrund der Leseprobe...]

[61] Streng wörtlich genommen macht die Formulierung „**voraussichtlich** ein hohes Risiko“ (engl. „**is likely** to result in a high risk“) möglicherweise nicht viel Sinn. Denn das Risiko ist per Definition das Produkt aus Wahrscheinlichkeit und Schadensschwere (siehe Wikipedia). Das Wort „voraussichtlich“ hätte man sich also sparen können.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 14).

6.1.1 Allgemeine Informationen zur Pflicht [GVO_035]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Im Bundesdatenschutzgesetz (in der neuen Fassung ab dem 25.05.2018) wird durch § 38 Abs. 1 BDSG die Benennung eines Datenschutzbeauftragten notwendig, sobald sich die Notwendigkeit einer Datenschutz-Folgenabschätzung ergibt. Dies betrifft die Pflicht **[GVO_037]** auf Seite 235.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Bayern stellt eine 23-seitige Orientierungshilfe zur Verfügung, die aber letztlich nur eine Risikopotential-Analyse beinhaltet und drei Methoden-Vorschläge liefert (SDM, PIA und britisches Modell) ● Liechtenstein stellt eine MS-Excel-Tabelle zur Prüfung zur Verfügung ● Die Datenschutz-PRAXIS 03/2020 berichtet auf Seite 8-11 und verweist u.a. auf die Bayerische Anleitung (siehe hier) ● Die ZD 09/2019 berichtet über die Schwierigkeiten und Unwägbarkeiten der Datenschutz-Folgenabschätzung auf Seite 390-394 ● Die Datenschutz-PRAXIS 09/2018 berichtet ausführlich auf Seite 6-9. ● DuD 08/2018 auf Seite 492-496 (ohne Praxisrelevanz). ● Das Workingpaper „WP 248“ der ehemaligen Artikel-29-Datenschutzgruppe liegt nun endlich auch in deutscher Sprache vor. ● DSK-Kurzpapier-18 erklärt Risiken und fordert eine DaSFA vorab für jede Verarbeitung ● Zeitschrift PinG 01/2018 Seite 26-30 und 30-40 und 41-43 ● Die GDD-Praxishilfe DS-GVO X (begründet ausführlich, dass die DaSFA nicht für bestehende Verarbeitungen gilt) ● **VdS-Richtlinie 10010** (Seite 512) im dortigen Kapitel 10.11 („Datenschutz-Folgenabschätzung“) ● 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 DSK-Kurzpapier-5 ● Die Aufsichtsbehörde Rheinland-Pfalz veröffentlichte 2013 eine 11-seitige Handreichung.

[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 DIN ISO 31000 zum Risikomanagement interessant sein (englisch, 134 €).

➔ Konkrete Beispiele für die Risiken hinsichtlich der „Rechte und Freiheiten“ finden sich auf Seite 451.

[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.]

6.2 Konsultation der Aufsichtsbehörde [GVO_036]

Datenschutz-Folgenabschätzung und Konsultation

Gemäß Artikel 36 muss das Unternehmen die Aufsichtsbehörde konsultieren, wenn die Datenschutz-Folgenabschätzung - trotz aller Sicherheitsmaßnahmen - ein hohes (Rest-) Risiko zum Ergebnis hat.

Dieser Pflicht wird das Kürzel **[GVO_036]** zugeordnet (siehe Seite 14).

6.2.1 Allgemeine Informationen zur Pflicht [GVO_036]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

6.2.2 Was bedeutet diese Pflicht [GVO_036] ?

Die zugrundeliegende Datenschutz-Folgenabschätzung wird im Rahmen der Pflicht **[GVO_035]** auf Seite 182 erklärt.

⚠ Diese Pflicht dürfte wohl **nur selten** zur Anwendung kommen. Denn wenn man die Aufsichtsbehörde wegen einem zu hohen (Rest-) Risiko kontaktiert, dann gibt man damit zu verstehen, dass man beim besten Willen keine angemessenen Sicherheitsmaßnahmen treffen kann. Nur die wenigsten Unternehmen werden sich selbst dieses Armutszeugnis ausstellen wollen.

Zum heutigen Zeitpunkt (August 2017) ist noch völlig unklar, wie man die Aufsichtsbehörde kontaktiert, und ob es entsprechende Meldeformulare geben wird. Es ist allerdings abzusehen, wie die Aufsichtsbehörden reagieren werden, denn sie sind nicht dafür bekannt, dass sie unbedingt eine pragmatische oder praxisorientierte Rechtsauffassung vertreten.

Eine Aufsichtsbehörde darf gemäß Erwägungsgrund 94 sogar eine geplante Datenverarbeitung untersagen, falls das (Rest-) Risiko zu hoch ist (siehe Seite 589).

Als Anlaufstelle für die Aufsichtsbehörde dient gemäß Artikel 39 (1e) der Datenschutzbeauftragte.

6.2.3 Wie erfüllt man diese Pflicht [GVO_036] ?

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: ● Binden Sie Ihren Datenschutzbeauftragten mit ein. ● Stellen Sie fest, welches die zuständige Aufsichtsbehörde ist. ● Stellen Sie der Aufsichtsbehörde Ihre Datenschutz-Folgenschätzung zur Verfügung. ● Befolgen Sie die Hinweise bzw. Anweisungen der Aufsichtsbehörde.

➔ Ein beispielhaftes Formular findet sich im Kapitel 12.18.4 auf Seite 461.

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 24.

☐ Eventuell machen Sie sich schon einmal vorab mit den Details einer „Konsultation“ vertraut. Denn wenn es akut wird, dann muss es schnell gehen. Die Konsultation muss erfolgen BEVOR die Datenverarbeitung beginnt. Sie müssen also auf eine Rückmeldung der Aufsichtsbehörde warten.

b) Durchführung („do“)

Wie führt man eine notwendige Konsultation der Aufsichtsbehörde durch?

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 25.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 Schadenersatzforderungen haften alle Verantwortlichen gemäß Artikel 82 (4) 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 des Daten-Transfers findet sich auf Seite 530.

Dieser Pflicht wird das Kürzel **[GVO_026]** zugeordnet (siehe Seite 14).

7.1.1 Allgemeine Informationen zur Pflicht [GVO_026]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente:
● Die 52-seitige EDPB-Guideline 2020-07 mit zahlreichen Aspekten zur gemeinsamen Verantwortlichkeit in den RdNr. 161-191 (mit automatisierter Übersetzung durch www.deepL.com) ● Das EDPB (siehe Seite 599) hat am 13.04.2021 einen 40-seitigen EDPB-Guideline 2020-08 zur „gezielten Ansprache von Nutzern sozialer Medien“ veröffentlicht (Herr Nicholas Vollmer hat für eine deutsche Übersetzung gesorgt.) ● Die GDD-Praxishilfe DS-GVO XV („JointControllership“) liefert theoretische Erläuterungen und eine Checkliste ● Datenschutz-Berater 05/2019 Seite 96-98 (wenig neue Erkenntnisse) ● ZD 02/2019 Seite 55-60 (wenig neue Erkenntnisse) ● Datenschutz-PRAXIS 02/2019 Seite 7-10 (auch hier werden gemeinsame Datenbestände bzw. Portale betont) ● Datenschutz-PRAXIS 01/2019 Seite 16-17 (allerdings ist es sehr fragwürdig, ob ein Fotograf ein gemeinsam Verantwortlicher ist). ● Die Datenschutzkonferenz nennt im Juni 2018 einen 8-Punkte-Fragenkatalog (anlässlich Facebook-Fanpage). ● Die ZD 09/2018 berichtet auf Seite 398-404 und liefert Ansätze für die Vertragsgestaltung. ● Der EuGH sieht facebook-Fanpage-Betreiber als gemeinsam Verantwortliche (siehe hier). ● Das DSK-Kurzpapier-16 [64] ● VdS-Richtlinie 10010 (Seite 512) im dortigen Kapitel 10.5 („Gemeinsam Verantwortliche“) ● 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.“*

[Ab hier eine Lücke aufgrund der Leseprobe...]

[64] Dieses DSK-Kurzpapier-16 liefert etwas rätselhafte Überlegungen zur „Funktionsübertragung“. Letztlich wird aber die „normale Übermittlung an einen Dritten“ thematisiert… ganz im Sinne des Kapitels 0 auf Seite 438.

7.2 EU-Vertreter benennen [GVO_027]

Andere Verantwortliche

Gemäß Artikel 27 (1) gilt eine besondere Pflicht für jene Verantwortlichen und Auftragsverarbeiter, die nicht innerhalb der EU niedergelassen sind: Sie müssen unter Umständen einen offiziellen „Vertreter“ innerhalb der EU benennen. Dieser Vertreter dient u.a. als Kontaktstelle für betroffene Personen und Aufsichtsbehörden.

Dieser Pflicht wird das Kürzel **[GVO_027]** zugeordnet (siehe Seite 14).

7.2.1 Allgemeine Informationen zur Pflicht [GVO_027]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

Diese Pflicht besteht aufgrund des „**Marktort-Prinzips**“ gemäß Artikel 3 (2); siehe Seite 615.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente. ● 9-seitige GDD-Praxishilfe DS-GVO XVIII im Dezember 2020 ● Datenschutz-PRAXIS 04/2019 Seite 15-17. ● RDV 06/2018 Seite 303-308 ● ZD 01/2019 Seite 14-18 (zur Haftung des EU-Vertreters).

[Im Rahmen von PrivazyPlan® wird das Dossier „Vertreter“ und 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.]

7.2.2 Was bedeutet diese Pflicht [GVO_027] ?

a) Wer ist betroffen?

Ein (außereuropäischer) Verantwortlicher muss den EU-Vertreter schriftlich Benennen, wenn

- die Verarbeitung gemäß Artikel 3 (2) auch Personen in der EU betrifft, und
- das Unternehmen keine EU-Niederlassung im Sinne des Artikel 4 Nr. 16 hat.

Die Pflicht gilt gemäß Artikel 27 (2a) aber nicht, wenn die folgenden drei Voraussetzungen gegeben sind:

- es ist **keine** regelmäßige Verarbeitung, sondern sie erfolgt nur gelegentlich bzw. sporadisch bzw. ungeplant, und
- es ist **keine** umfangreiche Verarbeitung „sensibler Daten“ im Sinne des Artikel 9 (1) bzw. Artikel 10 (mit anderen Worten: Es sind – wenn überhaupt welche - nur wenige Personen mit ihren sensiblen Daten betroffen), und
- es besteht **kein** hohes Risiko für die Rechte und Freiheiten der betroffenen Personen (sodass auch keine Datenschutz-Folgenabschätzung gemäß Artikel 35 notwendig ist).

In vielen Fällen dürften diese obigen Ausnahmen **keine** Anwendung finden, weil die Dienstleister ein Produkt anbieten, welche regelmäßig (also z.B. täglich) genutzt wird. Wenn es also darum geht, dass ein EU-Verantwortlicher einen US-Dienstleister als Auftragsverarbeiter beauftragen will, so dürfte dies eine regelmäßige Tätigkeit darstellen. Demnach könnte die Benennung eines EU-Vertreters notwendig sein.

Die Pflicht gilt gemäß Artikel 27 (2b) nicht für Behörden und öffentliche Stellen mit Sitz außerhalb der EU.

Es würde nicht überraschen, wenn zunächst viele kleine Dienstleister außerhalb Europas an dieser Pflicht scheitern würden (weil sie entweder diese Pflicht nicht kennen oder nicht wissen, wen sie benennen könnten, oder weil die Kosten einer solchen Benennung wirtschaftlich nicht tragbar sind).

b) Welche Aufgaben hat der EU-Vertreter?

Der Erwägungsgrund 80 legt fest, dass der Vertreter als Anlaufstelle für die Aufsichtsbehörde dient; vergleichbar dem betrieblichen Datenschutzbeauftragten gemäß Artikel 39 (1e). Er soll auch in Bezug auf aufsichtsbehördliche Maßnahmen mit den Aufsichtsbehörden zusammenarbeiten. Außerdem soll der (außereuropäische) Verantwortliche den Vertreter damit beauftragen, dass dieser in Bezug auf die Datenschutzpflichten handelt.

Alles in Allem sind die konkreten Aufgaben leider so vage formuliert, dass sich daraus kaum ein konkreter Dienstvertrag formulieren ließe. Die Funktion liegt irgendwo zwischen einem Boten und einem Stellvertreter.

[Ab hier eine Lücke aufgrund der Leseprobe...]

7.3 Auftragsverarbeitung detailliert regeln [GVO_028]

Andere Verantwortliche

Gemäß Artikel 28 kann der Verantwortliche externe Dienstleister einbinden, um personenbezogene Daten dort verarbeiten zu lassen. Geschieht dies streng weisungsgebunden, so spricht man von einer Auftragsverarbeitung („Outsourcing“). Für diese Offenlegung von Daten bedarf es keiner Einwilligung durch die betroffenen Personen; der Auftragsverarbeiter (siehe Artikel 4 Nr. 8) ist gemäß Artikel 4 Nr. 10 kein Dritter! Allerdings entsteht ein großer bürokratischer Aufwand, bevor eine Auftragsverarbeitung rechtskonform durchgeführt werden kann.

➔ Ein Überblick über alle Arten des Daten-Transfers findet sich auf Seite 530.

Dieser Pflicht wird das Kürzel **[GVO_028]** zugeordnet (siehe Seite 14).

7.3.1 Allgemeine Informationen zur Pflicht [GVO_028]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Die 52-seitige EDPB-Guideline 2020-07 mit zahlreichen Aspekten zur Auftragsverarbeitung in den RdNr. 93-160 (mit automatisierter Übersetzung durch www.deepL.com) ● die 20-seitige GDD-Praxishilfe DS-GVO IV („Mustervertrag zur Auftragsverarbeitung“) ● Eine 10-seitige FAQ zur Auftragsverarbeitung aus Niedersachsen mit konkreten Einschätzungen zu Spezialfällen ● Die „Datenschutz PRAXIS“ 08/2018 berichtet auf Seite 15-17 sehr ausführlich über Datenschutz in Microsoft Azure. ● **VdS-Richtlinie 10010** (siehe Seite 512) im dortigen Kapitel 12 („Auftragsverarbeitung“) ● Das DSK-Kurzpapier-13 ● Ein **Guide** der ico in Englisch ● Das Kurzpapier-10 der Bayerischen Aufsichtsbehörde ist lesenswert. ● Die GDD hat am 31.03.2017 die 23-seitige Praxishilfe IV (Vertragsmuster zur Auftragsverarbeitung) veröffentlicht. ● Konkrete Vertragsbeispiele finden sich im Unterkapitel 7.3.3...

[Im Rahmen von PrivazyPlan® wird das Dossier „Auftragsverarbeitung“ 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.]

7.3.2 Was bedeutet diese Pflicht [GVO_028] ?

In einer modernen Dienstleistungsgesellschaft ist es nicht ungewöhnlich, dass ein Verantwortlicher seine personenbezogenen Daten durch externe Dienstleister verarbeiten lässt. Dies nennt man **Auftragsverarbeitung** bzw. umgangssprachlich „Outsourcing“.

Woran erkennt man eine Auftragsverarbeitung? Die Bayerische Datenschutz-Aufsichtsbehörde hat dazu eine recht ausführliche **Liste an Beispielen** [70] veröffentlicht; dort wird auf Seite 2 interessanterweise auch aufgezählt, was KEINE Auftragsverarbeitungen sind (siehe auch Seite 531). Im Kapitel 7.2 des TOM-Guide® findet sich eine sehr ausführliche Checkliste, um eine Auftragsverarbeitung zu identifizieren.

➔ Eine Checkliste mit beispielhaften **Kriterien** einer Auftragsverarbeitung findet sich auf Seite 382.

In Deutschland regelt u.a. der § 80 SGB X (Sozialgesetzbuch) den Datenschutz der Gesundheits-, Renten- und Arbeitslosenversicherung. Der Wortlaut wurde auf die DS-GVO angepasst. Die PinG 05/2018 berichtet auf Seite 189 bis 197.

[Ab hier eine Lücke aufgrund der Leseprobe...]

[70] Funktioniert der Hyperlink nicht? Dann liegt es eventuell am MS-Internet-Explorer. Bitte verwenden Sie einen anderen Webbrowser, oder gehen Sie hier auf die Rubrik „Fragen und Antworten“ und klicken dann auf „Abgrenzung Auftragsverarbeitung“.

7.4 Auftragsverarbeitung streng nach Weisung durchführen [GVO_028a]

Andere Verantwortliche

Gemäß Artikel 28 (3) Satz 1 darf der Auftragsverarbeiter nur die vertraglich vereinbarten Verarbeitungen durchführen („Zwecke und Mittel"). Der Artikel 28 (3a) fordert ebenfalls „dokumentierte Weisungen". Der Auftragsverarbeiter muss also „Dienst nach Vorschrift" leisten. Bei genauer Betrachtung birgt diese Regelung Sprengstoff in sich. Die hier vorliegende Pflicht interpretiert dies aus Sicht des Auftragsverarbeiters.

Dieser Pflicht wird das Kürzel **[GVO_028a]** zugeordnet (siehe Seite 14).

7.4.1 Allgemeine Informationen zur Pflicht [GVO_028a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: Besonders hervorzugeben ist das Workingpaper „WP 169" der Artikel-29-Datenschutzgruppe.

[Im Rahmen von PrivazyPlan® wird das Dossier „Auftragsverarbeitung (Auftragnehmer)" 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.]

7.4.2 Was bedeutet diese Pflicht [GVO_028a] ?

Relevant ist auch der Artikel 29 (der dem Verantwortlichen eine Weisungsbefugnis hinsichtlich der Beschäftigten des Auftragsverarbeiters einräumt). Hierauf wird in der Schulungsreiche „Fit für die Datenschutz-Grundverordnung" im Januar 2017 auf Seite 5 hingewiesen; es wird auch betont, dass sich dies auch auf alle anderen (Unter-) Auftragsverarbeiter bezieht und vorsichtshalber in den Verträgen erwähnt werden sollte.

➔ Die wichtige Fragestellung nach der Präzision von Weisungen wird in einer („Express"-) Checkliste auf Seite 392 thematisiert.

a) Die Frage nach der Verantwortung

Schon immer war der Auftragsverarbeiter an die genauen Weisungen des Auftraggebers gebunden (siehe auch § 11 Abs. 2 Nr. 2 BDSG-alt). Doch wurde dies in der gelebten Praxis oftmals nicht wirklich ernst genommen. Nicht selten gab es nur allgemeinste Weisungen für den Auftragsverarbeiter. Bei so manchen Diensten diente sogar das Handbuch (bzw. die Onlinehilfe) als Weisung. All dies war zwar nicht zulässig, doch wurde es nur selten bemängelt und führte fast nie zu Geldbußen.

Auch im Rahmen von EU-Standarddatenschutzklauseln wurden die notwendigen Auftragsdetails in den Anhängen nur sehr oberflächlich ausgefüllt. Niemand kümmerte sich wirklich darum.

All dies könnte sich im Rahmen der DS-GVO elementar ändern. Wenn der Auftragsverarbeiter nämlich eine konkrete Verarbeitung durchführt, ohne dass sie im Sinne des Artikel 28 (3) Satz 1 dokumentiert wurde, dann handelt er auf eigene Verantwortung. Er wird diesbezüglich also zum „*Verantwortlichen*" gemäß Artikel 4 Nr. 7, weil er streng genommen die „*Zwecke und Mittel*" selbst bestimmt. Siehe weiter unten.

Das hat weitreichende Auswirkungen, wie der Artikel 28 (10) zeigt; im Schadensfall wird es zu einem „Hauen und Stechen" zwischen Auftraggeber und Auftragsverarbeiter führen, weil man insbesondere gemäß Artikel 82 (4) für Schadenersatzforderungen gemeinschaftlich haftet (siehe Seite 588). [75]

Der Nutznießer von vertraglichen Lücken (bzw. Verarbeitungen ohne konkrete Weisung) ist oftmals der Auftraggeber, weil er die Verantwortung im Schadensfall auf den Auftragsverarbeiter (ganz oder teilweise) abwälzen kann. Der Auftragsverarbeiter müsste dann die Geldbuße zahlen, und den Schadenersatz leisten und „seine" Datenschutzverstöße der Aufsichtsbehörde melden.

[Ab hier eine Lücke aufgrund der Leseprobe...]

[75] Der Gola-Kommentar geht (auf nur 8 Seiten Kommentierung zum Artikel 28) auf diese Sachlage nicht ausreichend ein. Auch Paal/Pauly thematisieren dies nicht wirklich in RdNr. 39ff zu Artikel 28. Der Kommentar von Kühling/Buchner deutet die Konsequenzen in RdNr. 65 zu Artikel 28 immerhin an.

7.5 Auftragsdatenverarbeitung aus BDSG übernehmen [GVO_028b]

Andere Verantwortliche

Bestehende Verträge zur Auftragsverarbeitung müssen am 25.05.2018 auf die neuen Anforderungen des Artikel 28 (3) überführt werden. Können die bestehenden Dienstleister hinreichende Garantien gemäß Artikel 28 (1) bieten?

Dieser Pflicht wird das Kürzel **[GVO_028b]** zugeordnet (siehe Seite 14).

7.5.1 Allgemeine Informationen zur Pflicht [GVO_028b]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

7.5.2 Was bedeutet diese Pflicht [GVO_028b] ?

Fast jeder Verantwortliche in Europa hat Teile seiner Datenverarbeitung auch schon vor dem 25.05.2018 im Rahmen von Outsourcing an externe Unternehmen ausgelagert. Im Idealfall hat er die datenschutzrechtliche Eignung geprüft und die notwendigen Verträge geschlossen (in Deutschland gemäß § 11 Abs. 2 BDSG-alt).

Doch egal, wie gut die Vergangenheit geregelt war: Ab dem 25.05.2018 gelten neue Regeln und neue Maßstäbe. Die hier vorliegende Pflicht **[GVO_028b]** stellt sicher, dass alle bis dahin bestehenden Outsourcing-Verträge auf den Prüfstand kommen.

Im Grunde genommen macht es keinen Unterschied, ob es sich um eine bestehende oder um eine neue Auftragsverarbeitung handelt. Insofern sind sämtliche Überlegungen der Pflicht **[GVO_028]** auf Seite 207 auch bei der hier vorliegenden Pflicht relevant.

a) Hinreichende Garantien

Gemäß Artikel 28 (1) müssen Auftragsverarbeiter hinreichende Garantien dafür bieten, dass sie geeignete technisch-organisatorische Maßnahmen so durchführen, damit **(a)** die Verarbeitung im Einklang mit der Verordnung erfolgt und **(b)** der Schutz der Rechte und Freiheiten der betroffenen Personen gewährleistet ist.

Insofern sind bestehende Konzepte, Testate und Zertifikate auf die neuen Anforderungen der DS-GVO zu prüfen.

➔ Ein beispielhaftes Formular zur Anbieter-Auswahl findet sich im Kapitel 12.14.4 auf Seite 385.

b) Vertragliche Umstellung

Die bestehenden Verträge müssen zum 25.05.2018 gekündigt werden. Die neuen Verträge gelten ab dem 25.05.2018. Selbstverständlich kann man in den neuen Verträgen regeln, dass eventuelle Rückgaben von Datenträgern und Löschungen von Daten beim Auftragnehmer NICHT durchgeführt werden müssen.

➔ Ein beispielhaftes Formular für eine solche Vertrags-Checkliste findet sich im Kapitel 12.14.5 auf Seite 387.

7.5.3 Wie erfüllt man diese Pflicht [GVO_028b] ?

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: ● Erstellen Sie eine Liste aller bestehenden Auftragsdatenverarbeitungen. ● Prüfen Sie, ob die bestehenden Dienstleister nach wie vor datenschutzrechtlich geeignet sind. ● Schließen Sie einen neuen Datenschutzvertrag gemäß Artikel 28 (3) ab. ● ➔ Nutzen Sie die Beispielformulare ab Seite 379.

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

[Ab hier eine Lücke aufgrund der Leseprobe...]

7.6 Datentransfer an Drittländer ist stark reglementiert [GVO_044]

Andere Verantwortliche

Gemäß der Artikel 44, 45, 46, 47, 48 und 49 ist ein Transfer von personenbezogen Daten an Drittländer bzw. internationale Organisationen streng reglementiert. Dies ist wichtig, weil die Daten den EU-Rechtsraum verlassen und danach nicht mehr „kontrolliert“ werden können.

Dieser Pflicht wird das Kürzel **[GVO_044]** zugeordnet (siehe Seite 14).

7.6.1 Allgemeine Informationen zur Pflicht [GVO_044]

Datentransfer an Drittländer ist stark reglementiert

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (5c) mit **hohen Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente, u.a. ● 18-seitige Handreichung der Stiftung Datenschutz vom 19.11.2022 beschreibt Internationale Datentransfers sehr umfassend und übersichtlich ● 16-seitige Ausarbeitung „DSGVO und Nutzung US-amerikanischer Cloud-Dienste“ des wissenschaftlichen Dienstes des Deutschen Bundestags am 03.06.2021 ● 14-seitige Orientierungshilfe aus Baden-Württemberg zum Schrems-II-Urteil am 04.09.2020 ● Bayerisches Arbeitspapier im Oktober 2018. ● Datenschutz-PRAXIS 04/2018 Seite 8-12. ● den 66-Leitfaden des BITKOM (deutsch, englisch) ● das DSK-Kurzpapier-4 ● den extrem ausführlichen Fachartikel in „Zeitschrift für Datenschutz“ 11/2017 Seite 503-509 (siehe hier).

[Im Rahmen von PrivazyPlan® wird das Dossier „Übermittlung an Drittländer bzw. internationale Organisationen“ 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.]

7.6.2 Was bedeutet diese Pflicht [GVO_044] ?

Datentransfer an Drittländer ist stark reglementiert

Bis zum 16.07.2020 war diese Pflicht im Rahmen des EU-US-PrivacyShield bzw. duch eine Unterzeichnung der seinerzeit gültigen EU-Standardvertragsklauseln (scheinbar) zu erfüllen. Doch dann kam das EuGH-Urteil Az. C311/18 (siehe Seite 496). Eine ausführliche Analyse und Todo-Liste finden Sie ab Seite 496.

In der EuGH-Pressemeldung vom 16.07.2020 sieht der EuGH die Datenschutz-Aufsichtsbehörden explizit **dazu verpflichtet, dass sie unrechtmäßige Drittland-Datentransfers aussetzen und verbieten müssen**. Insofern sind die oben genannten Geldbußen eine reale Gefahr. Dementsprechend kündigen im Juni 2021 viele deutsche Datenschutz-Aufsichtsbehörden eine „koordinierte Prüfung internationaler Datentransfers“ an (z.B. hier). Es sind also Untersagungen und Bußgelder zu befürchten (siehe Seite 575). Im Februar 2022 haben sich die europäischen Aufsichtsbehörden ca. 80 öffentliche Stellen kontaktiert um die Nutzung von Cloud-Diensten in Erfahrung zu bringen.

Die wunderbare Welt des (US-) Cloud-Computings (siehe Seite 662) hat für europäische Organisationen einen tiefen Riss erfahren.

➔ Passen Sie Ihre „Digitale Strategie“ an (siehe Seite 658) !!

Generell beachten Sie bitte folgende Kapitel:

➔ Das EuGH-Urteil C-311/18 im Juli 2020 zum EU-US-PrivacyShield und den „alten“ EU-Standardvertragsklauseln bringt den weltweiten Datentransfer ins Wanken.

➔ Die Drittland-Datentransfers werden erläutert auf Seite 533 und 534.

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 Geldbußen und Schadenersatzforderungen entscheidend minimiert, denn er stellt die notwendige Fachkompetenz zur Verfügung.

Dieser Pflicht wird das Kürzel **[GVO_037]** zugeordnet (siehe Seite 14).

8.1.1 Allgemeine Informationen zur Pflicht [GVO_037]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In Deutschland thematisiert der § 22 Abs. 2 Nr. 4 BDSG die Benennung eines Datenschutzbeauftragten im Gesundheits- und Sozialbereich (siehe Seite 283).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● RDV 04/2019 auf Seiten 176-180 zu zahlreichen Aspekten ● GDD-Praxishilfe DS-GVO I zum Datenschutzbeauftragten ● GDD-Ratgeber (Rund um den DSB, 2. Auflage, 133 Seiten) ● Baden-Württemberg liefert 64 Seiten an Information ● Ausführliche Hinweise in der ULD-Praxisreihe 2 auf 16 Seiten. ● 12-seitige Broschüre des ULD ● 24-seitige FAQ der NRW-Aufsichtsbehörde ● DSK-Kurzpapier-12 ● Die 30-seitige Workingpaper „WP 243“ der Artikel-29-Datenschutzgruppe.

Im Dezember 2019 verhängte der Bundesdatenschutzbeauftragte ein Bußgeld von 10.000 € gegen ein Kleinstunternehmen, welches sich beharrlich weigerte einen Datenschutzbeauftragten zu benennen.

➔ Ein beispielhaftes Formular findet sich im Kapitel 12.19 auf Seite 464. 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 464):

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. Im Autohaus werden mitunter hohe Rabatte für schwerbehindere Personen gewährt, aber diese Verarbeitung ist (gemäß telefonischer Abstimmung mit einer Aufsichtsbehörde) wohl eher nicht als Kerntätigkeit zu werten. Die Patientendaten im Krankenhaus sind hingegen eine Kerntätigkeit.

Gemäß Erwägungsgrund 24 ist beispielsweise das Nachvollziehen von Internetaktivitäten eine Verhaltensbeobachtung oder nutzungsbezogene Profilbildung.

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.2 Bekanntmachung des Datenschutzbeauftragten [GVO_037a]

Datenschutzbeauftragten benennen

Gemäß Artikel 37 (7) ist die Existenz (und Kontaktmöglichkeiten) des Datenschutzbeauftragten bekannt zu machen. Somit haben sowohl die betroffenen Personen (als auch die Aufsichtsbehörde) jederzeit die Möglichkeit einer Kontaktaufnahme. Eine fehlende Benennung bleibt somit nicht unbemerkt.

Dieser Pflicht wird das Kürzel **[GVO_037a]** zugeordnet (siehe Seite 14).

8.2.1 Allgemeine Informationen zur Pflicht [GVO_037a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

8.2.2 Was bedeutet diese Pflicht [GVO_037a] ?

Die geforderte Bekanntmachung hat verschiedene Aspekte:

1.) **Bekanntmachung an Betroffene**
Der Verantwortliche muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen. Dies wird wohl in aller Regel über das Internet geschehen. Idealerweise würde dies auf einer „Datenschutz"-Seite geschehen; falls diese nicht existiert, so würde die „Impressum"-Seite und/oder „Kontakt"-Seite ausreichen.
Falls das Unternehmen über keine eigene Website verfügt, so könnte man die Kontaktdaten u.a. in der Fußzeile der E-Mails bekanntmachen.
Wie detailliert muss diese Veröffentlichung ausfallen? Eine funktionsbezogene E-Mail-Adresse (also ohne den Namen) kann möglicherweise ausreichen. Die Aufsichtsbehörde in Baden-Württemberg nennt konkrete Details. Trotzdem kann es ratsam sein, den vollen Namen zu veröffentlichen; gemäß Kühling/Buchner in RdNr. 37f zu Artikel 37 stelle dies eine vertrauensbildende Maßnahme dar, die dazu führe, dass betroffene Personen sich direkt an das Unternehmen wenden, statt sich sofort bei der Aufsichtsbehörde zu beschweren. Das ist ein sehr gutes Argument.

2.) **Mitteilung an Aufsichtsbehörden**
Der Verantwortliche muss die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitteilen. Die Mitteilungs-Formulare finden Sie hier.

Im Februar 2020 wurde ein Bußgeld von 51.000 € gegen die deutsche Niederlassung von facebook verhängt, weil ein Wechsel des Datenschutzbeauftragten nicht gemeldet wurde.

Muss auch ein **freiwillig benannter** Datenschutzbeauftragter mitgeteilt werden? Der Wortlaut der DS-GVO macht diesbezüglich keinen Unterschied. Die Aufsichtsbehörde in Schleswig-Holstein verlangt keine Meldung von freiwillig benannten DSBs. Eine interessante Diskussion findet sich hier.

Es gibt Stimmen, die behaupten, dass die Aufsichtsbehörden diese Meldungen auch dahingehend auswerten, ob es externe Datenschutzbeauftragte gibt, die massenweise Mandate zu Dumpingpreisen sammeln (in diesen Fällen ist der Ärger mit der Aufsichtsbehörde programmiert).

Diese Regelung erfüllt einige wichtige Zwecke:

- **Vertrauensbildende Maßnahme**
  Wenn die betroffenen Personen sehen, dass der Verantwortliche einen Datenschutzbeauftragten bestellt hat, so wird man den Produkten bzw. Dienstleistungen möglicherweise mehr Vertrauen entgegenbringen. Das führt zu mehr Kunden und mehr Umsatz.

- **Eventuell weniger Beschwerden bei den Aufsichtsbehörden**
  Es wird den betroffenen Personen sehr leichtfallen, den Datenschutzbeauftragten zu kontaktieren. Dies kann verhindern, dass sich die Betroffenen als Erstes bei der Aufsichtsbehörde melden. Insofern kann eine (teure, weil zeitintensive) Beschwerde bei der Aufsichtsbehörde zunächst vermieden werden. Insofern sollten nicht nur die Kontaktdaten gemeldet werden, sondern der volle Name des Datenschutzbeauftragten.
  Ein zusätzlicher Satz kann dies verstärken: „*Sie haben eine Beschwerde bezüglich des Datenschutzes in unserem Unternehmen? Dann können Sie unseren Datenschutzbeauftragten kostenlos kontaktieren*".

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.3 Frühzeitige Einbindung des Datenschutzbeauftragten [GVO_038]

Datenschutzbeauftragten benennen

Gemäß Artikel 38 (1) muss der Verantwortliche den Datenschutzbeauftragten präzise und frühzeitig einbinden. Somit ist der Datenschutzbeauftragte immer auf dem Laufenden und kann seine Expertise optimal einbringen.

Dieser Pflicht wird das Kürzel **[GVO_038]** zugeordnet (siehe Seite 14).

8.3.1 Allgemeine Informationen zur Pflicht [GVO_038]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

8.3.2 Was bedeutet diese Pflicht [GVO_038] ?

Der DSB ist also aktiv in die Geschäftsprozesse einzubinden. Dies betrifft die Ebene der Geschäftsmodelle, der Geschäftsprozesse und teilweise sogar das Tagesgeschäft (Beschwerden, Auftragsverarbeitungen, Website-Gestaltung). Die folgenden Beispiele sollen das verdeutlichen:

- neue Softwareprodukte sollen im Unternehmen eingesetzt werden, wobei möglicherweise eine vorherige Datenschutz-Folgenabschätzung notwendig sein könnte
- neue Dienstleister sollen Zugriff auf die personenbezogenen Daten haben, um bestimmte Arbeiten damit zu erledigen (Auftragsverarbeitung)
- neue Technologien sollen eingesetzt werden (z.B. eine Chat-Funktion auf der Website), wobei das Unternehmen oftmals die genauen Details dieser Technologien nicht kennt
- neue Videoüberwachungen sollen installiert werden, um beispielsweise Diebstahl und Sachbeschädigungen zu dokumentieren (bzw. potenzielle Täter abzuschrecken)
- Datenschutzverletzungen wurden festgestellt, weil personenbezogene Daten z.B. per E-Mail an falsche Empfänger versendet wurden
- betroffene Personen beschweren sich
- die Aufsichtsbehörde nimmt Kontakt mit dem Verantwortlichen auf
- und vieles mehr…

Der Verantwortliche muss in allen Datenschutz-Fragen frühzeitig an den Datenschutzbeauftragten denken. Wichtig sind die folgenden Aspekte:

1.) **Ordnungsgemäß einbinden**
Der Datenschutzbeauftragte muss ordnungsgemäß (engl. „properly“ im Sinne von präzise, richtig, korrekt, exakt, ordentlich) eingebunden werden. Es reicht also nicht aus, wenn der DSB nur grob und vage quasi pro forma eingebunden wird.
Diese Forderung der DS-GVO wird jeder Datenschutzbeauftragte begrüßen. Auf der Basis von umfangreichen und präzisen Informationen kann er viel schneller und präziser seine Beratung leisten.
Beispiel: Ein Unternehmen plant auf der Website ein Chat-Modul einzubinden. Der US-amerikanische Hersteller bietet hierfür ein simpel einzubindendes JavaScript an. Da hier personenbezogene Kommunikationsdaten verarbeitet (und in den USA gespeichert) werden, besteht eine hohe Datenschutzrelevanz. Der Datenschutzbeauftragte muss über diese Verarbeitung **präzise informiert** werden:
- Welche Daten werden erhoben (IP-Adresse, Chat-Protokolle, Datei-Anhänge, Videobilder, …)?
- Erfolgt die Datenübertragen durchweg verschlüsselt?
- Wann werden die Daten wieder gelöscht?
- Hält der US-amerikanische Anbieter die DS-GVO ein? Sofern Artikel 3 (2) greift.
- Welche Datenschutz-Garantien liefert der US-amerikanische Anbieter?
- und vieles mehr.

Ein anderer Aspekt der „Ordnungsmäßigkeit“ kann die **Form der Einbindung** betreffen. Bei komplexen Fragestellungen (wie dem obigen Beispiel) ist es hilfreich, wenn die Informationen in Schriftform an den Datenschutzbeauftragten weitergegeben werden.

2.) **Frühzeitig einbinden**
Der Datenschutzbeauftragte muss frühzeitig eingebunden werden. Die Erfahrung zeigt, dass die Verantwortlichen dies in der Vergangenheit nicht immer berücksichtigten. Das hatte durchaus konkrete Auswirkungen: Manchmal war der Datenschutzbeauftragte die letzte Person im Unterneh-

8.4 Unterstützung des Datenschutzbeauftragten [GVO_038a]

Datenschutzbeauftragten benennen

Gemäß Artikel 38 (2) hat der Verantwortliche den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Die erforderlichen Ressourcen (Zeit, Geld, Räumlichkeiten, Unterstützung durch die Fachabteilungen) müssen nachweisbar zur Verfügung gestellt werden.

Dieser Pflicht wird das Kürzel **[GVO_038a]** zugeordnet (siehe Seite 14).

8.4.1 Allgemeine Informationen zur Pflicht [GVO_038a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

8.4.2 Was bedeutet diese Pflicht [GVO_038a] ?

Damit der Datenschutzbeauftragte seine Aufgaben gemäß Artikel 39 erfüllen kann, unterstützt ihn der Verantwortliche durch:

- **Erforderliche Ressourcen**
  Dieser sehr weite Begriff umfasst zunächst ein abgeschlossenes Büro und technische Kommunikationsmittel (Telefon, E-Mail, etc.) und die Möglichkeit auch vertrauliche Dinge zugriffsgeschützt zu speichern. Auch finanzielle Mittel sind bereitzustellen, um beispielsweise Hilfsmaterialien (wie z.B. den PrivazyPlan®) zu kaufen. Natürlich sind auch personelle Ressourcen wichtig: Die Fachabteilungen werden immer wieder fachliche Zuarbeiten leisten müssen; dies muss in der betrieblichen Planung einbezogen werden. Der Datenschutzbeauftragte benötigt zur Erfüllung seiner Aufgaben natürlich auch eigene Arbeitszeit; sofern ein interner Datenschutzbeauftragter bestellt wird, so muss die beschäftigte Person wohl von anderen Aufgaben entbunden werden.

- **Zugang zu den personenbezogenen Daten und Verarbeitungsvorgängen**
  Dem Datenschutzbeauftragten darf der Zugang zur Datenverarbeitung nicht verwehrt werden. Der notwendige Zugriff auf Daten, Software und Hardware muss sichergestellt sein. Die Gespräche mit den Fachabteilungen darf nicht eingeschränkt werden.

- **Erhaltung des Fachwissens**
  Sofern ein **interner** Datenschutzbeauftragter benannt wird, so kostet die Erhaltung des datenschutzrechtlichen Fachwissens Zeit und Geld. Zunächst ist für die notwendige Fachliteratur zu sorgen (also Zeitschriften, Bücher und Onlinequellen, siehe Seite 518). Auch der TOM-Guide® kann in dieser Hinsicht eine wichtige Rolle spielen. Ebenso sind regelmäßige externe Fortbildungen sicherzustellen. Und nicht zuletzt muss für die Erhaltung der Fachkunde auch großzügig Arbeitszeit eingeplant werden; die DS-GVO ist sehr komplex, und es dauert nicht selten einige Stunden, bis ein spezielles Detail sicher verstanden wurde.
  Im Falle eines **externen** Datenschutzbeauftragten wird die benannte Person sich selbstständig um diese Aspekte kümmern. Hier wird der Verantwortliche einen gewissen Nachweis einfordern dürfen.

Die entscheidende Ressource ist wohl die **Zeit**. Der Datenschutzbeauftragte muss sich in die juristischen und technischen Aspekte des Datenschutzes einarbeiten. Und er muss die ca. 50 Pflichten des Verantwortlichen verstehen, um diesbezüglich zu unterrichten und zu beraten. Hinzu kommen die ca. 5 eigenen DSB-Pflichten des Kapitels 11 ab Seite 294. Je nach persönlichen Voraussetzungen kann dies gut und gerne zwei Monate exklusiver Beschäftigung mit diesen Themen bedeuten.

8.4.3 Wie erfüllt man diese Pflicht [GVO_038a] ?

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: ● Zusammen mit dem Datenschutzbeauftragten werden die benötigten Ressourcen festgelegt. ● Dem Datenschutzbeauftragten ist ausreichend Zeit einzuräumen, damit er die Fachkunde erlangen und aktualisieren kann. ● Nutzen Sie den PrivazyPlan®.

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

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.5 DSB als Anlaufstelle für betroffene Personen [GVO_038b]

Datenschutzbeauftragten benennen

Gemäß Artikel 38 (4) haben die betroffenen Personen das Recht auf einen uneingeschränkten Zugang zum Datenschutzbeauftragten. Dies muss der Verantwortliche sicherstellen.

Dieser Pflicht wird das Kürzel **[GVO_038a]** zugeordnet (siehe Seite 14).

8.5.1 Allgemeine Informationen zur Pflicht [GVO_038a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

[Im Rahmen des PrivazyPlan® wird das Dossier „Beschwerde“ 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.]

➔ Die dazugehörige Pflicht **[DSB_005]** des Datenschutzbeauftragten wird auf Seite 305 erläutert.

8.5.2 Was bedeutet diese Pflicht [GVO_038b] ?

Die DS-GVO ändert die Sachlage insofern, als das die Existenz und die konkreten Kontaktdaten des Datenschutzbeauftragten an verschiedenen Stellen bekannt gemacht werden: **(a)** im Rahmen der Veröffentlichungspflicht des Artikel 37 (7) und **(b)** im Rahmen der Datenerhebung (bei Dritten) gemäß Artikel 13 (1b) und Artikel 14 (1b).

Insofern ist es möglich, dass die betroffenen Personen sich im Rahmen der DS-GVO öfter mal beim Datenschutzbeauftragten melden. Dies ist in gewisser Hinsicht sehr zu begrüßen: Je geringer die Schwelle zur Kontaktierung des Datenschutzbeauftragten ist, desto unwahrscheinlicher ist es, dass sich die betroffenen Personen sofort bei der Aufsichtsbehörde beschweren. Eine Eskalation kann somit wohl oft vermieden werden.

8.5.3 Wie erfüllt man diese Pflicht [GVO_038b] ?

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: ● Legen Sie fest, wie die Kontaktaufnahmen der betroffenen Personen gehandhabt werden sollen.

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 24.

☐ Sollen die Kontakte mit betroffenen Personen durch den Datenschutzbeauftragten **separat dokumentiert** werden? Somit könnte der Datenschutzbeauftragte z.B. im Rahmen seines Jahresberichts diese Kontakte aufzählen. Somit hat die Geschäftsleitung einen guten Überblick über die Außenwirkung, und außerdem hat der Verantwortliche eine gute Grundlage für Nachweise gegenüber der Aufsichtsbehörde.

☐ Der **zeitliche Aufwand** für den Datenschutzbeauftragten ist vorab kaum einzuschätzen. Insbesondere bei externen Datenschutzbeauftragten ist eine diesbezügliche pauschale Vergütung schwer zu beziffern. Insofern könnte man hier einen geringen monatlichen Pauschalbetrag vereinbaren (z.B. eine Stunde monatlich) und den darüberhinausgehenden Aufwand gegen Nachweis separat vergüten.

☐ Inwieweit ist bei Funktion als „Anlaufstelle“ eine **Rücksprache mit der Fachabteilung** erwünscht? Insbesondere bei externen Datenschutzbeauftragten sind derlei Überlegungen relevant. Möglicherweise soll der Datenschutzbeauftragte erst mal nur das Anliegen der betroffenen Personen aufnehmen, um

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.6 Unterrichtung und Beratung hinsichtlich der Pflichten [GVO_039]

Datenschutzbeauftragten benennen

Gemäß Artikel 39 (1a) muss der Datenschutzbeauftragte den Verantwortlichen bezüglich dessen Datenschutz-Pflichten unterrichten und beraten. Seitens des Verantwortlichen müssen dafür die Voraussetzungen geschaffen und der Erfolg kontrolliert werden.

Dieser Pflicht wird das Kürzel **[GVO_039]** zugeordnet (siehe Seite 14).

8.6.1 Allgemeine Informationen zur Pflicht [GVO_039]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

➔ Die dazugehörige Unterrichtungs-Pflicht **[DSB_001]** des Datenschutzbeauftragten wird auf Seite 298 erläutert.

➔ Die dazugehörige Beratungs-Pflicht **[DSB_002]** des Datenschutzbeauftragten wird auf Seite 299 erläutert.

8.6.2 Was bedeutet diese Pflicht [GVO_039] ?

Im Kern betrifft diese Pflicht vor allem den Datenschutzbeauftragten selbst (siehe Seite 298). Doch was kann der Verantwortliche dazu beitragen?

- **Explizite Aufgabenzuweisung**
  Ganz konkret sollte der Datenschutzbeauftragte im Rahmen seiner Benennung zumindest auf die folgenden Aufgaben hingewiesen werden:

  1.) Identifizierung der Datenschutz-Pflichten
  Der Datenschutzbeauftragte muss von sich heraus aktiv die wichtigsten Pflichten aus der DS-GVO (und anderer Rechtsvorschriften) herausarbeiten. Nur so kann es funktionieren. Der Verantwortliche kann ja nicht warten, bis er von einer betroffenen Person der einer Aufsichtsperson auf seine Pflicht (-Verletzung) hingewiesen wird.

  2.) Unterrichtung zu den Pflichten
  Die Unterrichtung (engl. „to inform“ im Sinne von informieren) sorgt dafür, dass der Verantwortliche überhaupt einmal von seinen Pflichten Kenntnis erlangt. Im Idealfall wird der Datenschutzbeauftragte die jeweilige Pflicht benennen und erklären.
  Darüber hinaus sollte der Datenschutzbeauftragte auch über alle Neuerungen informieren, damit der Verantwortliche insgesamt auf dem Stand der Dinge ist: Gibt es neue Gesetze oder Verordnungen? Sind im Internet neue Leitlinien oder Hinweistexte zu finden? Haben die Aufsichtsbehörden oder die Artikel-29-Datenschutzgruppe neue rechtliche Einschätzungen veröffentlicht?

  3.) Beratung zu den Pflichten
  Die Beratung (engl. „to advise“ im Sinne von beraten, empfehlen) sorgt dafür, dass der Verantwortliche nicht völlig auf sich allein gestellt ist. Denn allein eine erfolgte Unterrichtung zu den Pflichten führt noch nicht automatisch dazu, dass der Verantwortliche auch die notwendigen Schritte unternehmen kann, um die Einhaltung der Pflichten in Angriff zu nehmen.
  Die Beratungsleistung des Datenschutzbeauftragten hat wohl mindestens zwei Aspekte: **(a)** eine allgemeine Beratung zur jeweiligen Pflicht ganz im Sinne des hier vorliegenden PrivazyPlan® und **(b)** eine laufende Beratung im betrieblichen Alltag zu allen Fragen, die die beteiligten Beschäftigten haben werden.

- **Passende Auswahl eines Datenschutzbeauftragten**
  Der Verantwortliche sollte schon bei der Auswahl eines Datenschutzbeauftragten darauf achten, dass jener den oben beschriebenen Unterrichtungs- und Beratungspflicht nachkommen kann (und will). Es wäre unerfreulich, wenn sich im Rahmen der Zusammenarbeit herausstellen würde, dass der Datenschutzbeauftragte gänzlich andere Prioritäten setzt.

- **Kontrollieren des Datenschutzbeauftragten**
  Bei aller Fachkompetenz des Datenschutzbeauftragten: Die Unternehmensleitung kann nicht einfach blind darauf vertrauen, dass er den oben genannten Unterrichtungs- und Beratungspflicht nachkommt. Die Compliance-Verantwortung liegt letztlich bei der Unternehmensleitung. Frei nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“.
  - Bezüglich der **Unterrichtungs-Pflicht** könnte der Datenschutzbeauftragte

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.7 Überwachung der Einhaltung von Datenschutzvorschriften [GVO_039a]

Datenschutzbeauftragten benennen

Gemäß Artikel 39 (1b) hat der Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften zu überwachen. Dies umfasst auch die Überwachung der Strategien (Zuweisung von Zuständigkeiten, Mitarbeiterschulungen, Audits, etc.). Seitens des Verantwortlichen müssen dafür die Voraussetzungen geschaffen und der Erfolg kontrolliert werden.

Dieser Pflicht wird das Kürzel **[GVO_039a]** zugeordnet (siehe Seite 14).

8.7.1 Allgemeine Informationen zur Pflicht [GVO_039a]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

➔ Die dazugehörige Überwachungs-Pflicht **[DSB_002]** des Datenschutzbeauftragten wird auf Seite 300 erläutert.

8.7.2 Was bedeutet diese Pflicht [GVO_039a] ?

Im Kern betrifft diese Pflicht vor allem den Datenschutzbeauftragten selbst (siehe Seite 300). Doch was kann der Verantwortliche dazu beitragen?

- **Explizite Aufgabenzuweisung**
  Ganz konkret sollte der Datenschutzbeauftragte im Rahmen seiner Benennung zumindest auf die folgenden Aufgaben hingewiesen werden:

  1.) Überwachung der Regeltreue
  Die Überwachung der Einhaltung [85] dieser Verordnung ist explizit anzuweisen.
  Im Kern läuft dies primär auf die Überwachung der ca. 50 Pflichten der DS-GVO (und ggf. anderer Rechtsvorschriften) hinaus. Zusammen mit dem Datenschutzbeauftragten sollte also ein Pflichten-Überwachungsplan erarbeitet werden. Im einfachsten Fall wird sich der Datenschutzbeauftragte jede Woche eine Pflicht vornehmen und deren Einhaltung im Unternehmen des Verantwortlichen prüfen. Da das Kalenderjahr ca. 52 Wochen hat, kann der Datenschutzbeauftragte im Laufe eines Jahres (fast) alle Pflichten einmal überwacht haben. Zugegeben: Dieser Ansatz ist vielleicht ungewöhnlich… aber er ist pragmatisch.

  2.) Überwachung der Strategien [86]
  Die Überwachung der Strategien (engl. „monitor the policies“) sollte als Aufgabe für den Datenschutzbeauftragten formuliert werden. Wobei dies nur dann konkret zum Tragen kommt, wenn der Verantwortliche überhaupt irgendwelche überwachbaren Strategien (Policies) formuliert hat (siehe Satz 2 im Erwägungsgrund 78). Ohne schriftlich formulierte Policies gibt es für den Datenschutzbeauftragten nicht viel zu überwachen (außer festzustellen, dass solche Policies nicht existieren).
  Diese Strategien für den Schutz personenbezogener Daten könnten beispielsweise umfassen:
  - Zuweisung von Zuständigkeiten
  - Sensibilisierung und Schulung der Beschäftigten, die das Unternehmen durchführt
  - Auditierungen („Überprüfungen“), denen sich das Unternehmen unterwirft.
  Vielleicht ist hiermit auch gemeint, dass zu überwachen sei, inwieweit der Verantwortliche selbst seine Strategie-Einhaltung überprüft.

- **Passende Auswahl eines Datenschutzbeauftragten**
  Der Verantwortliche sollte schon bei der Auswahl eines Datenschutzbeauftragten darauf achten, dass er den oben beschriebenen Unterrichtungs-

[85] Der Begriff „Überwachung“ basiert auf engl. „monitor compliance“ im Sinne von kontrollieren, beaufsichtigen, überprüfen. Es wird sicherlich noch viele Diskussionen darüber geben, wie dieser Begriff konkret interpretiert werden soll.

[86] ACHTUNG: Bezüglich des Artikel 39 (1b) gibt es Schwierigkeiten bei der Interpretation. Manche Autoren lesen heraus, dass der Datenschutzbeauftragte irgendwelche Weisungs- oder Schulungs-Befugnisse hätte. So auch die Information des Hessischen Landes-Datenschutzbeauftragten: Er führt ohne weitere Begründung den Begriff „Kontrolle“ ein und schreibt: „Der Datenschutzbeauftragte kann daher auch Einfluss auf die organisatorische Umsetzung des Datenschutzrechts nehmen“.
Das erscheint abwegig. Solange nicht von offizieller Seite eine derartige Interpretation vorgegeben wird, gehen wir hier davon aus, dass sämtliche Belange vom Datenschutzbeauftragten lediglich „passiv“ überwacht werden.

[Ab hier eine Lücke aufgrund der Leseprobe...]

8.8 Anlaufstelle für Aufsichtsbehörde und Zusammenarbeit [GVO_039b]

Datenschutzbeauftragten benennen

Gemäß Artikel 39 (1e) dient der Datenschutzbeauftragte als Anlaufstelle (engl. „*contact point*“) der Aufsichtsbehörde. Diesbezüglich ist er gemäß Artikel 39 (1d) generell zur Zusammenarbeit (engl. „*cooperation*“) mit der Aufsichtsbehörde verpflichtet. Insofern werden in dem hier vorliegenden Kapitel zwei Literale zu einer Pflicht zusammengeführt.

Dieser Pflicht wird das Kürzel **[GVO_039b]** zugeordnet (siehe Seite 14).

8.8.1 Allgemeine Informationen zur Pflicht [GVO_039b]

Die Aufsichtsbehörde kann Verstöße gemäß Artikel 83 (4a) mit **Geldbußen** ahnden (siehe Seite 575). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen (und ggf. Schadenersatzforderungen, siehe Seite 582) abzuwehren oder zumindest abzumildern.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente.

[Im Rahmen des PrivazyPlan® wird das Dossier „Beschwerde“ 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.]

➔ Die dazugehörige Überwachungs-Pflicht **[DSB_004]** des Datenschutzbeauftragten wird auf Seite 305 erläutert.

8.8.2 Was bedeutet diese Pflicht [GVO_039b] ?

Im Kern betrifft diese Pflicht vor allem den Datenschutzbeauftragten selbst (siehe Seite 305). Doch was kann der Verantwortliche dazu beitragen?

- Die **Kontaktaufnahme** durch die Aufsichtsbehörde ist insofern kein Problem, weil der Verantwortliche ihr die Kontaktdaten des Datenschutzbeauftragten gemäß Artikel 37 (7) bereits gemeldet hatte.
  Hier sollte es niemanden geben, der sich dazwischenschaltet. Es wäre also unzulässig, wenn die Geschäftsführung beispielsweise die telefonische Durchwahl des Datenschutzbeauftragten nicht nennt und ein Anrufer immer erst über die Geschäftsleitung gehen müsste.

- Die **Zusammenarbeit** von Aufsichtsbehörde und Datenschutzbeauftragtem bedeutet auch, dass es in den gemeinsamen Telefonaten oder im Schriftverkehr keine „Zensur“ durch das Unternehmen geben darf.
  Das ist nicht trivial. Jeder erfahrene Datenschutzbeauftragte kennt das mulmige Gefühl, wenn er direkt mit der Aufsichtsbehörde kommuniziert. Ein einziges falsches Wort kann über Geldbußen entscheiden (die das betreute Unternehmen dann zu zahlen hat). Hier muss ein Kompromiss gefunden werden zwischen den Unternehmens-Interessen und der Zusammenarbeits-Pflicht des Datenschutzbeauftragten.

8.8.3 Wie erfüllt man diese Pflicht [GVO_039b] ?

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: ● Der Datenschutzbeauftragte wird angewiesen, dass er von der Aufsichtsbehörde direkt kontaktiert wird. ● Die Art der Zusammenarbeit zwischen Datenschutzbeauftragtem und Aufsichtsbehörde wird geregelt. ● Kontrollieren Sie den Datenschutzbeauftragten diesbezüglich.

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 24.

☐ Soll der Datenschutzbeauftragte im Rahmen seiner **Tätigkeitsdokumentation** alle Kontakte mit der Aufsichtsbehörde dokumentieren? Somit könnte dies im Rahmen seines Jahresberichts erscheinen.

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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.

Die DS-GVO gilt unter bestimmten Umständen auch für Unternehmen außerhalb Europas (siehe Seite 615). Der Stand der weltweiten Datenschutz-Gesetzgebung wurde am 08.01.2018 hier publiziert.

9.1 Europa (Verordnungen, Richtlinien, Konventionen)

Sonstige Datenschutzvorschriften

Das europäische Recht spielt (spätestens seit dem Jahr 2016) eine immer wichtigere Rolle im Datenschutz.

Das EU-Parlament behandelt zum Thema „Digitalisierung“ ca. 50 Entwürfe für Richtlinien/Verordnungen (siehe auch hier). Die Digitalisierung wird ganz offensichtlich in Brüssel entschieden. Es werden also in den nächsten Jahren noch zahlreiche neue Reglementierungen zu erwarten sein.

9.1.1 EU-Verordnungen

Die EU-Verordnungen sind unmittelbar anwendbares Recht. Die nationalen Parlamente müssen also keine entsprechenden Gesetze erlassen. Die EU wählt dieses Instrument immer dann, wenn europaweit ein einheitliches Niveau erzwungen werden soll. Mitunter gibt es „Öffnungsklauseln“, die es den Nationalstaaten gewisse Anpassungen erlauben.
Die im Folgenden aufgeführten EU-Verordnungen werden nach ihrem Datum sortiert.

a) EU 2016/679 - Datenschutz-Grundverordnung !!!

Aufgrund dieser Verordnung ist der PrivazyPlan® entstanden.
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 609.

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**.

b) EU 2018/1725 – für EU-Organe

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union. Insofern ist dies für dies für die Privatwirtschaft NICHT relevant.

9.1.2 Richtlinien

Die EU-Richtlinien sind Handlungsaufforderungen an die nationalen Parlamente. Brüssel gibt somit vor, welche Rechtsvorschriften die Staaten zu erlassen haben. So muss beispielsweise das deutsche Telemediengesetz (TMG) an die ePrivacy-Richtlinie angepasst werden (bzw. rechtslinienkonform ausgelegt werden).

[Ab hier eine Lücke aufgrund der Leseprobe...]

9.1.3 EU-Konventionen

Von gewissem Interesse können auch die völkerrechtlichen Konventionen sein.

a) EU-Rats-Konvention 108

Die hier thematisierte Konvention ist keine Rechtsvorschrift, doch soll sie trotzdem erwähnt werden, weil sie als eine „kleine Schwester" der DS-GVO gilt. Siehe hier und hier. Die finale Fassung findet sich hier. Als Unterzeichner gelten derzeit u.a. Argentinien, Marokko, Mexiko, Tunesien und Uruguay.

Warum ist das von Bedeutung? Angesichts der problematischen Situation hinsichtlich der **EU-Standarddatenschutzklauseln** nach dem EuGH-Urteil (siehe Seite 224 und Seite 496) kann man vermutlich sagen: Die Unterzeichnung dieser Konvention kann als zusätzliche Garantie dafür gelten, dass ein EU-konformer Datenschutz im Drittland auch auf staatlicher Ebene gewährleistet ist (siehe Seite 472).

Würden auch die USA diese Konvention unterzeichnen, so wären viele Probleme gelöst.

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 609).

Das kann für jeden Verantwortlichen große Auswirkungen haben, sofern er personenbezogene Daten in EU-weiten Niederlassungen verarbeitet.

Derzeit ist keine Website bekannt, wo Brüssel die neuen Datenschutzgesetze der jeweiligen EU-Staaten bekannt macht. Das ist sehr unerfreulich. Es bleibt zu hoffen, dass dies bis zum 25.05.2018 nachgeholt wird. Die EU-Kommission könnte u.a. die folgenden Mitteilungspflichten zum Anlass nehmen, um diese nationalen Rechtsvorschriften zu publizieren: Artikel 51 (4), Artikel 83 (9), Artikel 84 (2), Artikel 88 (3) und Artikel 90 (2).

Im Folgenden nennen wir die neuen Datenschutzgesetze der EU-Mitgliedsstaaten, sofern sie uns bekannt sind. Allerdings übernehmen wir keine Garantie für die Richtigkeit/Vollständigkeit.

9.2.1 Belgien

Belgien hat am 03.12.2017 ein neues Datenschutzgesetz erlassen [C – 2017/31916]. Mit 114 Artikeln auf umgerechnet 8 Seiten ein recht umfassendes Werk.

9.2.2 Deutschland

In Deutschland wurde am 30.06.2017 das DSAnpUG-EU verkündet (siehe Seite 266). Es umfasst viele verschiedene Gesetze auf insgesamt 36 Seiten.

In Bayern hat der Ministerrat am 05.06.2018 u.a. beschlossen, dass **(a)** durch Ehrenamt getragene Vereine etc. keinen Datenschutzbeauftragten benennen müssen und **(b)** bei einem Erstverstoß im Dickicht der Datenschutzregeln keine Geldbußen drohen, sondern Hinweise und Beratung Vorrang vor Sanktionen haben und **(c)** Abmahnanwälte mit rechtsmissbräuchlichen Abmahnungen (siehe Seite 590) nicht hingenommen werden.

In Deutschland wurden viele Gesetze aufgrund der DS-GVO novelliert. Eine Liste findet sich hier.

Ein neues „Gesetz zum Schutz von Geschäftsgeheimnissen" (GeschGehG) wurde am 18.04.2019 erlassen (siehe hier und hier). Das kann relevant sein, wenn es darum geht, dass gemäß Erwägungsgrund 63 keine solche Geheimnisse im Rahmen einer Datenkopie ausgeliefert werden (siehe Pflicht **[GVO_015a]** auf Seite 58). Die §§17-19 UWG fallen somit weg. Siehe auch hier und DuD 09/2019 auf Seite 569-574.

9.2.3 Dänemark

Dänemark hat seit dem 17.05.2018 ein neues Datenschutzgesetz. Der Gesetzestext findet sich eventuell hier.[88]

[88] Das Wort „eventuell" wird an dieser Stelle genutzt, weil wir nicht sicher einschätzen können, ob die genannten Hyperlinks wirklich stimmen. Dafür fehlt uns die Sprachkenntnis.

[Ab hier eine Lücke aufgrund der Leseprobe...]

9.3 Kirchengesetze

Sonstige Datenschutzvorschriften

Gemäß Artikel 91 können Kirchen und religiöse Vereinigungen oder Gemeinschaften eigene Datenschutzvorschriften erlassen.

In Deutschland haben die Kirchen reagiert (in beiden Fällen sind immaterielle Schadenersatzforderungen und Geldbußen bis zu 500.000 € möglich):

- Die Katholische Kirche hat am 20.11.2017 das „Gesetz über den Kirchlichen Datenschutz (KDG)“ beschlossen, welches am 25.05.2018 wirksam wird. Es umfasst 58 Paragrafen auf 48 Seiten.

- Die Evangelische Kirche hat am 15.11.2017 das neue „Kirchengesetz über den Datenschutz in der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) beschlossen. Es umfasst 56 Paragrafen auf 37 Seiten.

Siehe RDV 01/2018 Seite 8-13. Siehe Datenschutz-Berater 09/2018 auf Seite 179-181.

Eine Textsammlung mit allen relevanten Regelwerken bietet das Buch „Kirchliches Datenschutzrecht“ von Alexander Golland (2. Auflage, 2020, 340 Seiten, 35 €).

9.4 Deutsche Gesetze

Sonstige Datenschutzvorschriften

In Deutschland gibt es neben der DS-GVO auch andere Datenschutzvorschriften, aus denen Pflichten resultieren. Einige Beispiele dafür sind:

9.4.1 BDSG ab dem 25.05.2018

Deutsche Gesetze

In Deutschland gilt ab dem 25.05.2018 das komplett überarbeitete Bundesdatenschutzgesetz („BDSG“). Im Kapitel 10 ab Seite 277 werden die Pflichten des BDSG beschrieben.

Das seit 1997 existierende Bundesdatenschutzgesetz tritt gemäß Artikel 8 DSAnpUG-EU außer Kraft.

Den Wortlaut haben wir unter www.bdsg2018.de publiziert. Seit Juni 2018 gibt es auch den offiziellen BDSG-Gesetzestext (u.a. auch in Englisch).

9.4.2 Landes-Datenschutzgesetze

Deutsche Gesetze

Für die öffentlichen Stellen der Bundesländer gelten u.a. auch die jeweiligen eigenen Datenschutzgesetze (siehe hier und hier). Die Wechselwirkungen dieser Landesdatenschutzgesetze mit der DS-GVO und dem BDSG sind nicht trivial.

Für einige Landesdatenschutzgesetze gibt es eigene Kommentare: Baden-Württemberg, Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz.

Alle Landesdatenschutzgesetze verstehen sich explizit als „**Ergänzung**“ zur EU DS-GVO (2016/679) und zur EU Justiz-Verordnung (2016/680).

In Bezug auf das **BDSG** finden sich hingegen nur sporadische Einzel-Verweise. Der § 1 Abs. 1 Nr. 2 BDSG ist wohl eher bedeutungslos, weil alle Landesdatenschutzgesetze an die DS-GVO angepasst wurden.

In Hinblick auf den § 26 BDSG (**Beschäftigtendaten**) besagt das DSK-Kurzpapier-14:

> *„Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes und Länder – einschließlich der Kommunen – gelten besondere bundes- und landesspezifische Regelungen (z.B. beamtenrechtliche Vorschriften). Die Regelungen des § 26 BDSG finden dann keine Anwendung.“*

[Ab hier eine Lücke aufgrund der Leseprobe...]

in der Ausgabe 02/2019 auf Seite 1-4. Demnach sieht es im Rahmen der DS-GVO folgendermaßen aus:

- Für **Unternehmer** ist das KunstUrhG irrelevant, weil es keine entsprechende Öffnungsklausel gibt. Als Rechtsgrundlage gelten ersatzweise zum Beispiel der Artikel 6 DS-GVO oder der § 26 BDSG (siehe Kapitel „Datenverarbeitungen brauchen eine Rechtsgrundlage [GVO_006]“ ab Seite 122). [92]

- Für **Journalisten** ist die Öffnungsklausel des Artikel 85 (1) relevant und insofern gilt das KUG weiterhin. Dementsprechend gilt die „weiche“ Pflicht **[AUX_006]** nur noch für Journalisten (siehe Seite 322). Siehe Urteil des OLG Köln, Az. I-15 W 27/18 vom 18.06.2018.

- Für **Privatpersonen** gilt die DS-GVO nicht und insofern wird der § 22 KunstUrhG unverändert angewendet. Siehe Urteil des OLG Oldenburg, Az. 13 W 10/18 vom 24.05.2018.

e) Telekommunikationsgesetz (TKG)

Mit der Einführung des TTDSG wurde das TKG von allen datenschutzrechtlichen Aspekten befreit.

Siehe aber die „weiche“ Pflicht **[AUX_002]** („Regelung zur Privatnutzung“) auf Seite 319.

f) Patientendaten-Schutz-Gesetz (PDSG)

Anlässlich der Telematik-Infrastruktur wurde in Deutschland ein PDSG neu verabschiedet; es handelt sich um ein „Artikelgesetz“, welches zahlreiche Gesetzesänderungen umfasst. Bezüglich des SGB 5 gibt es zahlreiche Änderungen auf 48 Seiten (im § 307 SGB 5 werden die datenschutzrechtlichen Verantwortlichkeiten definiert... hier ist relevant die „*dezentrale Infrastruktur bestehend aus Komponenten zur Authentifizierung und zur sicheren Übermittlung von Daten in die zentrale Infrastruktur*“ [93]). Das Apothekengesetz wird auf Seite 48 novelliert. Im Bundesgesetzblatt findet man die Veröffentlichung hier.

[92] ~~Die Hamburger Aufsichtsbehörde teilt diese Auffassung, denn sie sieht hier im Mai 2018 keine Anwendung des § 22 KuG außerhalb des Journalismus.~~

[93] Experten kritisieren die Tatsache, dass ein niedergelassener Arzt für die Kartenlesegeräte und die Verschlüsselung der Datenübermittlung verantwortlich sein soll: Wie soll denn ein Arzt diese Geräte und Software beeinflussen können?

Der zuständige Bundesdatenschutzbeauftragte hatte schon während der Beschlussphase auf Datenschutzmängel hingewiesen und sieht sich gezwungen gegen die Krankenkassen rechtliche Maßnahmen zu treffen (... einmal mehr ist erkennbar, dass der Gesetzgeber gerne ins datenschutzrechtliche Risiko geht).

Eine Zusammenfassung der Besonderheiten von Berufsgeheimnisträgern findet sich auf Seite 619.

g) Datenschutz, Telekommunikation und Telemedien (TTDSG)

Ab dem 01.12.2021 wird in Deutschland das neue TTDSG gelten (siehe Seite 495). Daraus ergeben sich zwei neue Pflichten, die bis Dezember 2021 hier im PrivazyPlan® eingearbeitet werden:

- **Jugendschutz-Daten nicht kommerziell nutzen [TTDSG_020]**
  Diese Forderung ist auch schon vor dem 01.12.2021 im § 14a TMG enthalten, allerdings ohne konkrete Bußgeld-Androhung. ➔ Seite 274

- **Cookies etc. benötigen (in aller Regel) eine Einwilligung [TTDSG_025]**
  Diese Forderung wurde bisher vom BGH in den § 15 Abs. 3 TMG hineingelesen, auch wenn dies dem Wortlaut krass widersprach (siehe Seite 261). Nun endlich – nach 12 Jahren – hat der deutsche Gesetzgeber eine Formulierung gefunden, die dem Artikel 5 E-Privacy-Richtlinie entspricht. Nun ist ein Verstoß bußgeldbewehrt. ➔ Seite 274

Aus dem TTDSG ergibt sich in Deutschland außerdem die Pflicht zur Benennung einer verantwortlichen „Fachkraft für Behörden-Auskünfte“ (siehe Seite 322).

9.5 Rechtsvorschriften in Drittländern

Sonstige Datenschutzvorschriften ▲

9.5.1 US-Amerikanisches Datenschutzrecht

Die USA befanden sich datenschutzrechtlich von jeher eher auf der „**passiven**“ Seite (in dem Sinne, dass eine Datenübermittlung dorthin nicht immer einwand-

[Ab hier eine Lücke aufgrund der Leseprobe...]

frei rechtmäßig stattfand... siehe Seite 496). Doch nun erscheinen die USA auch auf der „**aktiven**“ Seite, indem der Staat Kalifornien den EU-Unternehmen Auflagen macht.

Kalifornien verschärft das Datenschutzrecht ab dem Jahr 2022

Zu den „sonstigen Datenschutzvorschriften“ für EU-Unternehmen gehört nun auch das der „California Privacy Rights Act“ (**CPRA**) in den USA. Ab Januar 2022 wird es (auch für manche EU-Unternehmen) ernst.

Dies ist für EU-Unternehmen relevant, sofern sie **(a)** mit US-Unternehmen verbunden sind, **(b)** mehr als 25 Mio. Euro Jahresumsatz machen, **(c)** mehr als 100.000 Kalifornische Einwohnerdaten verarbeiten, oder **(d)** mehr als 50% des Jahresumsatzes mit Datenhandel erzielen.
Es kann also schon ausreichen, dass täglich mehr als 274 Kalifornier die Firmen-Website besuchen.

Die zahlreichen kalifornischen Datenschutz-Spezialgesetze werden nun also auch von einer US-Datenschutz-Aufsichtsbehörde überwacht. Es ist ein Novum, dass sich US-Bürger per Bürgerentscheid (im November 2020) für eine neue Behörde einsetzen. Für europäische Unternehmen gab es schon ab dem 01.01.2020 erhöhte Anforderungen durch den lange bestehenden „California Consumer Privacy Act“ (**CCPA**). Ab dem 01.01.2022 und 01.01.2023 kommen durch den CPRA neue Pflichten hinzu. Da erhebliche Geldbußen und Schadenersatzforderungen bestehen (siehe ab Seite 575) ist dies durchaus ein wichtiger Aspekt. Siehe Zeitschrift für Datenschutz 02/2021 auf Seite 70-74.

⚠ Prüfen Sie rechtzeitig, ob Ihr Unternehmen die obigen Kriterien erfüllt. Falls Sie unter den **CPRA** fallen, so gibt es neue Pflichten zu erfüllen.
(Da dies in Deutschland wohl für die wenigsten Verantwortlichen zutrifft, haben wir auf eine Ergänzung der „weichen“ Pflichten auf Seite 319 verzichtet).

9.5.2 Chinesisches Datenschutzrecht

In China gilt ab dem 01.11.2021 ein neues Datenschutzrecht (siehe hier). Unter anderem ist ein Werbe-Widerspruch vorgesehen und eine Einwilligung bei der Verarbeitung von sensiblen Daten erforderlich. Falls ein europäisches Unternehmen den chinesischen Markt bedient, so muss ein Repräsentant vor Ort benannt werden (ähnlich der Pflicht **[GVO_027]** auf Seite 204) und es besteht die Pflicht zur Berichterstattung gegenüber den chinesischen Aufsichtsbehörden.

9.6 Sonstige Datenschutzpflichten in Deutschland

Sonstige Datenschutzvorschriften

Im PrivazyPlan® werden die bußgeldbewehrten Pflichten aus dem deutschen Recht hier zusammengefasst. Somit wird das Kapitel 9.4 etwas entlastet.

9.6.1 Berufliche Schweigepflicht [STGB_203]

Sonstige Datenschutzpflichten in Deutschland

In Deutschland darf ein Berufsgeheimnisträger gemäß § 203 StGB die ihm anvertrauten Daten nicht unbefugt offenbaren.

Eine Zusammenfassung der Besonderheiten von Berufsgeheimnisträgern findet sich auf Seite 619.

Siehe Kapitel 8.7 im TOM-Guide®. Die speziellen Aspekte zum Outsourcing durch einen Berufsgeheimnisträger sind im Kapitel 3.3.3h des TOM-Guide® ausführlich beschrieben. Siehe auch die Zeitschrift PinG 01/2018 Seite 16-20 und Seite 21-25 und 43-48. Siehe 17-seitige BITKOM-Anleitung vom Juli 2018 mit einer Verpflichtungserklärung für externe Gehilfen.

Sehr wichtig ist die StGB-Novellierung im Bundesgesetzblatt Teil I Nr. 71 vom 08.11.2017. Die Absätze 2a und 3 werden durch zwei neue Absätze 3 und 4 ersetzt (siehe hier). Die Beauftragung von Auftragsverarbeitern und Unter-Auftragsverarbeitern wurde legalisiert. Siehe TOM-Guide® im Kapitel 8.7.4. Im Falle von Rechtsanwälten kommt aber noch die Änderung des § 43e BRAO hinzu, die die Sachlage wohl verkompliziert (siehe „Zeitschrift für Datenschutz“ 11/2017 Seite 501).

Die Bayerische Datenschutz-Aufsichtsbehörde sieht bei der Namensnennung in einer ärztlichen Praxis (am Telefon oder im Wartezimmer) kein Problem. Es sei

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

10.0 Einleitung

BDSG

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 609).

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 518) 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 noch zu frisch, als dass abschließende Einschätzungen möglich wären.

10.0.1 Die neue Gesetzgebung („DSAnpUG-EU“)

Die DS-GVO regelt den Datenschutz nicht bis ins letzte Detail. Vielmehr gibt es ca. 80 Öffnungsklauseln, die den Staaten eigene Regelungen erlauben (siehe Seite 609). Sehr schön zusammengefasst wurde dies hier. Das neue BDSG ist in Deutsch und Englisch zu lesen.

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

a) Novellierungen im April 2017

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.

Vom BDSG sind für die Privatwirtschaft die Artikel 1 (ca. 75% von Teil 1 und Teil 2), Artikel 7 und Artikel 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 12 finden Sie verschiedene Möglichkeiten, wie Sie auf den Gesetzestext zugreifen können.

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

Falls Ihr Unternehmen gemäß § 4f BDSG-alt bereits einen Datenschutzbeauftragten bestellt hat, so finden Sie auf Seite 239 einige Hinweise, wie damit zukünftig umgegangen werden kann.

b) Novellierungen im Oktober 2018

In einem 563-seitigen Entwurf zur weitergehenden Anpassung des deutschen Datenschutzrechts an die DS-GVO sind über 150 deutsche Gesetze betroffen (u.a. das BDSG auf Seite 24 mit erstaunlich wenigen Änderungen).

Man hätte erwarten können, dass zumindest die Bestimmungen des § 4 BDSG zur Videoüberwachung überarbeitet worden wären, weil diese durchgängig als unrechtmäßig angesehen werden (siehe Pflichten **[BDSG_004]** und **[BDSG_004a]** ab Seite 280). Weit gefehlt.

Dieses 2. DSAnpUG-EU wurde am 25.11.2019 im Bundesgesetzblatt bekannt gemacht (siehe ZD 11/2020 Seite 556-561, wobei man sich fragen kann, warum über ein Gesetzesänderung berichtet wird, die 12 Monate her ist).

10.0.2 Gibt es Konflikte zwischen der DS-GVO und dem BDSG?

Allerdings. Die Fachwelt ist sich einig, dass der deutsche Gesetzgeber zu viel und zu lax regelt. Im Folgenden nennen wir nur jene Fälle, die im Rahmen des PrivazyPlan® eine Rolle spielen:

- § 4 BDSG (Videoüberwachung)
  Der deutsche Gesetzgeber erlaubt die Videoüberwachung, obwohl es dafür keine passende Öffnungsklausel gibt. Die Fachwelt ist sich einig, dass für die nicht-öffentlichen Stellen allein Artikel 6 die Rechtsgrundlage darstellen kann. Insofern greifen die Privilegierungen von Sportstätten und Busverkehr

[Ab hier eine Lücke aufgrund der Leseprobe...]

10.1 OBSOLET: Videoüberwachungen kenntlich machen

BDSG

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

Dieser Pflicht wird das Kürzel **[BDSG_004]** zugeordnet (siehe Seite 14).

➔ Siehe Seite 610, wo begründet wird, dass der § 4 BDSG keine Rechtsgrundlage **für die Videoüberwachung** liefern kann.

10.1.1 Allgemeine Informationen zur Pflicht [BDSG_004]

Die Aufsichtsbehörde kann auf den ersten Blick **keine Geldbuße** verhängen, weil im § 43 BDSG („Bußgeldvorschriften“) kein Bezug auf die Videoüberwachung genommen wird. Doch gemäß Artikel 83 (9) kann der gesamte Artikel 83 analog angewendet werden, wenn eine nationale Rechtsvorschrift keine Geldbußen vorsieht (siehe Seite 577).

Die **Fachliteratur** (siehe Seite 518) liefert verschiedene Hinweise: ● Die „Zeitschrift für Datenschutz“ 10/2018 Seite XV über EU-rechtswidrige Bestimmungen im BDSG. ● Die „Zeitschrift für Datenschutz“ 07/2018 Seite 345-347 über EU-rechtswidrige Bestimmungen im BDSG. ● Die Gesetzesbegründung bringt keine neuen Erkenntnisse. ● Kommentar von Kühling/Buchner (2. Auflage) in RdNr. 15 zu § 4 BDSG (der § 4 BDSG kommt in der Privatwirtschaft eher nicht zur Anwendung) und in RdNr. 172 zu Artikel 6 ● Kommentar von Gierschmann in RdNr. 256 zu Artikel 6 ● DSK-Kurzpapier-15 (hier wird der § 4 BDSG kaum erwähnt, weil er potentiell unionrechtswidrig sein könnte) ● Fachzeitschrift ZD 09/2017 Seite 407-411 (geht kaum auf das BDSG ein, weil die Regelungen als unionsrechtswidrig angesehen werden; ansonsten nur in Ausnahmefällen). ● Die Aufsichtsbehörde aus Niedersachsen liefert eine ausführliche Transparenz-Anleitung (als Downloads unten rechts; auch dort wird Artikel 6 (1f) als Rechtsgrundlage einer Videoüberwachung angesehen).

➔ Die Videoüberwachung wird im Kapitel 13.17 („Videoüberwachung“) auf Seite 622 behandelt.

10.2 OBSOLET: Identifizierte Personen von Videoüberwachung informieren [BDSG_004a]

BDSG

~~In Deutschland muss der Verantwortliche gemäß § 4 Abs. 4 BDSG die **Identifizierung** einer betroffenen Person im Rahmen einer öffentlich zugänglichen Videoüberwachung schnellstmöglich **mitteilen**. Somit hat die betroffene Person schnellstmöglich Kenntnis von diesem Umstand.~~

~~Dieser Pflicht wird das Kürzel **[BDSG_004a]** zugeordnet (siehe Seite 14).~~

➔ Siehe Seite 610, wo begründet wird, dass der § 4 BDSG keine Rechtsgrundlage **für die Videoüberwachung** liefern kann.

Dieses Kapitel wurde im Juli 2019 radikal gekürzt, weil es nicht mehr relevant ist.

10.3 Sicherheitsmaßnahmen bei sensiblen Daten [BDSG_022]

BDSG

In Deutschland müssen gemäß § 22 Abs. 2 BDSG angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorgesehen werden, sofern „besondere Kategorien“ von personenbezogenen Daten verarbeitet werden. Betroffen ist u.a. der Gesundheits- und Sozialbereich und generell jede Verarbeitung, die auf einer deutschen Rechtsgrundlage beruht.

Dieser Pflicht wird das Kürzel **[BDSG_022]** zugeordnet (siehe Seite 14).

10.3.1 Allgemeine Informationen zur Pflicht [BDSG_022]

Die Aufsichtsbehörde kann auf den ersten Blick **keine Geldbuße** verhängen, weil im § 43 BDSG („Bußgeldvorschriften“) kein Bezug auf diese Pflicht genommen wird. Doch gemäß Artikel 83 (9) kann der gesamte (Geldbuß-) Artikel 83 auch dann angewendet werden, wenn eine nationale Rechtsvorschrift keine Geldbußen vorsieht (siehe Seite 577).

Eine Zusammenfassung der Besonderheiten von Berufsgeheimnisträgern findet sich auf Seite 619.

In der **Fachliteratur** (siehe Seite 518) hilft weiter: ● DuD 09/2017 Seite 542. ● Der Fachkommentar Kühling/Buchner (2. Auflage) weist in RdNr. 27 zu § 22 Abs. 2 BDSG darauf hin, dass nur Verarbeitungen betroffen sind, die auf deutschen Rechtsgrundlagen beruhen. ● Die Gesetzesbegründung bringt keine neuen Erkenntnisse.

10.3.2 Was bedeutet diese Pflicht [BDSG_022] ?

Basierend auf dem § 22 Abs. 2 BDSG sind vier Szenarien zu beachten:

a) § 22 Abs. 1 BDSG
Im Rahmen des Gesundheitsbereichs (Sozialschutz, Gesundheitsvorsorge, öffentliche Gesundheit, Behandlungsvertrag mit Berufsgeheimnisträger - siehe Seite 124), mit denen der Artikel 9 (2h) ergänzt wird. Hier wird der gesamte Gesundheitsbereich abgedeckt, wie es auch schon im § 28 Abs. 7 BDSG-alt der Fall war.

b) § 27 Abs. 1 BDSG
Im Rahmen der Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken.

c) § 28 Abs. 1 BDSG
Im Rahmen von Datenverarbeitungen zu öffentlichen Archivzwecken.

d) § 37 Abs. 2 BDSG
Im Rahmen von zulässigen automatisierten Einzelfallentscheidungen im Falle von Leistungserbringungen von Versicherungsverträgen im Zusammenhang mit Gesundheitsdaten.

Der § 22 Abs. 2 BDSG stellt nun eine Mindestforderung von 10 „angemessenen und spezifischen“ Maßnahmen, die vom Verantwortlichen vorzusehen sind. Diese Forderungen erinnern etwas an die Anlage zu § 9 Satz 1 BDSG-alt.

Im Kern orientieren sich die Forderungen am Artikel 32 (1): „Sicherheit der Verarbeitung“, was gemäß der Pflicht **[GVO_032]** auf ein Informations-Sicherheits-Managementsystem (ISMS) hinausläuft (siehe Seite 158). Auch rein sprachlich ist man an den dazugehörigen Erwägungsgrund 83 erinnert (der ebenfalls die Implementierungskosten thematisiert).

Hinzu kommen aber mindestens die folgenden Aspekte (die der deutsche Gesetzgeber auch in der Gesetzesbegründung leider nicht weiter erläutert):

- **(Nr. 2)** Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben oder entfernt worden sind. Dies entspricht der „**Eingabekontrolle**“ aus der Anlage zum § 9 des alten BDSG-alt in der Nummer 5 (siehe Kapitel 2.5 im TOM-Guide®). Nimmt man diese Maßnahme wörtlich, dann ist die Eingabekontrolle eine sehr weitgehende Maßnahme, die die meisten Software-Produkte erfahrungsgemäß nicht vollständig erfüllen. Dies sollte bei den technisch-organisatorischen Maßnahmen gemäß der Pflicht **[GVO_032]** berücksichtigt werden (siehe Seite 158).

- **(Nr. 3)** Eine **Sensibilisierung** der an den Verarbeitungsvorgängen beteiligten Personen. Zusätzlich zu einer „normalen“ Datenschutz-Schulung soll also zusätzlich auch über die „besonderen Kategorien“ personenbezogener Da-

10.4 Sensible Forschungsdaten anonymisieren [BDSG_027]

BDSG

In Deutschland muss gemäß § 27 Abs. 3 BDSG bei der Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken dafür gesorgt werden, dass die „besonderen Kategorien" personenbezogener Daten a) zunächst gesondert gespeichert und dann b) schnellstmöglich anonymisiert werden.

Dieser Pflicht wird das Kürzel **[BDSG_027]** zugeordnet (siehe Seite 14).

10.4.1 Allgemeine Informationen zur Pflicht [BDSG_027]

Die Aufsichtsbehörde kann auf den ersten Blick **keine Geldbuße** verhängen, weil im § 43 BDSG („Bußgeldvorschriften") kein Bezug auf diese Pflicht genommen wird. Doch gemäß Artikel 83 (9) kann der gesamte (Geldbuß-) Artikel 83 analog angewendet werden, wenn eine nationale Rechtsvorschrift keine Geldbußen vorsieht (siehe Seite 577).

In der **Fachliteratur** (siehe Seite 518) hilft weiter: ● Die DuD 10/2018 berichtet auf Seite 640-646. ● Fachkommentar von Kühling/Buchner (2. Auflage) in RdNr. 23-24. ● DuD 05/2017 Seite 300-305. ● Die Gesetzesbegründung bringt keine neuen Erkenntnisse („*Absätze 3 und 4 sind § 40 Absatz 2 und 3 BDSG a. F. entlehnt.*").

10.4.2 Was bedeutet diese Pflicht [BDSG_027] ?

Im Kern soll dafür gesorgt werden, dass der Umgang mit Forschungsdaten sich durch die DS-GVO nicht ändert. Es wird die Öffnungsklausel des Artikel 89 (2) genutzt.

Im Kern gilt diese Regelung beispielsweise für die Markt- und Meinungsforschung. Es bleibt unverändert bei dem Grundsatz, dass Identifikationsmerkmale zu löschen sind, sobald dies nach dem Forschungs- bzw. Statistikzweck möglich ist.

Der § 27 Abs. 3 BDSG bezieht sich speziell auf „sensible" Daten (siehe Seite 616). Dies ist für die Forschung keine neue Forderung, sondern gelebte Praxis (und zwar auch für nicht-sensible Daten).

10.4.3 Wie erfüllt man diese Pflicht [BDSG_027] ?

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: ● Sensible Forschungsdaten sollten schnellstmöglich anonymisiert werden; notfalls reicht zwischenzeitlich eine Pseudonymisierung.

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 24.

b) Durchführung („do")

Wie soll diese Pflicht konkret erfüllt werden?

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 25.

☐ Anonymisieren die die sensiblen Daten frühestmöglich.

☐ Falls eine Pseudonymisierung (z.B. für langfristige Forschungen) notwendig ist, so ist dies zulässig. Dokumentieren Sie die Umstände. Stellen Sie sicher, dass keine unbefugten Personen auf diese Personen-Zuordnung zugreifen kann.

c) Überwachung („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 26.

10.5 Auskunftei muss EU-Darlehensgebern Auskunft geben [BDSG_030]

BDSG

In Deutschland muss gemäß § 30 Abs. 1 BDSG ein Kredit- oder Finanzierungsgeber die Auskunftsverlangen aus anderen EU/EWR Ländern genauso behandeln wie inländische Auskunftsverlangen.

Dieser Pflicht wird das Kürzel **[BDSG_030]** zugeordnet (siehe Seite 14).

10.5.1 Allgemeine Informationen zur Pflicht [BDSG_030]

Die Aufsichtsbehörde kann Verstöße gemäß § 43 Abs. 1 Nr. 1 BDSG mit **Geldbußen** von bis zu 50.000 € ahnden (siehe Seite 578). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen abzuwehren oder zumindest abzumildern.

Zugrunde liegt auch die Verbraucherkreditrichtlinie (VerbrKredRL) 2008/48/EG vom 23.04.2008, wo besonders der dortige Artikel 9 relevant ist.

In der **Fachliteratur** (siehe Seite 518) gibt es durchaus relevante Stellen: ● Der Kommentar von Däubler/Wedde/Weichert/Sommer auf Seite 1110-1112. ● Die Gesetzesbegründung bringt keine neuen Erkenntnisse.

10.5.2 Was bedeutet diese Pflicht [BDSG_030] ?

Eine EU-weite Gleichbehandlung von Auskunftsverlangen soll sichergestellt werden. Wenn Sie Verbraucherkredite vergeben, so müssen inländische und ausländische Verbraucher gleichbehandelt werden.

10.5.3 Wie erfüllt man diese Pflicht [BDSG_030] ?

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: ● Auskunftsverlangen von inländischen und ausländischen Personen sind gleichermaßen zu beantworten.

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 24.

☐ Prüfen Sie, ob Sie dieser Bestimmung unterliegen.

b) Durchführung („do")

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

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 25.

☐ Stellen Sie sicher, dass inländische und ausländische Verbraucher die gleiche Transparenz erfahren.

c) Überwachung („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 26.

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 27.

10.6 Abgelehnte Finanzierung muss Auskunftei als Grundlage nennen [BDSG_030a]

BDSG

In Deutschland muss gemäß § 30 Abs. 2 BDSG ein Kredit- oder Finanzierungsgeber die betroffene Person darüber unterrichten, wenn eine Ablehnung durch die negative Bonitätsauskunft einer Auskunftei herrührt.

Dieser Pflicht wird das Kürzel **[BDSG_030a]** zugeordnet (siehe Seite 14).

10.6.1 Allgemeine Informationen zur Pflicht [BDSG_030a]

Die Aufsichtsbehörde kann Verstöße gemäß § 43 Abs. 1 Nr. 2 BDSG mit **Geldbußen** von bis zu 50.000 € ahnden (siehe Seite 578). So gesehen ist die Erfüllung dieser Pflicht wichtig, um Geldbußen abzuwehren oder zumindest abzumildern.

Zugrunde liegt auch die Verbraucherkreditrichtlinie (VerbrKredRL) 2008/48/EG vom 23.04.2008, wo besonders der dortige Artikel 9 relevant ist.

In der **Fachliteratur** (siehe Seite 518) gibt es durchaus relevante Stellen: ● Der Kommentar von Däubler/Wedde/Weichert/Sommer auf Seite 1110-1112. ● Die Gesetzesbegründung bringt keine neuen Erkenntnisse.

10.6.2 Was bedeutet diese Pflicht [BDSG_030a] ?

Eine EU-weite Gleichbehandlung von abgelehnten Kreditnehmern soll sichergestellt werden. Wenn die Ablehnung eines Kredits oder einer Finanzierung (allein?) durch eine negative Bonitätsauskunft herrührt.

10.6.3 Wie erfüllt man diese Pflicht [BDSG_030a] ?

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: ● Informieren Sie die betroffenen Personen, wenn eine abgelehnte Finanzierung auf Auskunftei-Informationen beruht.

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 24.

☐ Die Vorschrift ist nur anzuwenden, wenn der Abschluss eines Verbraucherdarlehensvertrags (§ 491a Abs. 1 BGB) oder eines entgeltlichen Finanzierungshilfevertrags (§ 506 BGB) abgelehnt wird. [96]

b) Durchführung („do")

Wie soll diese Pflicht konkret erfüllt werden?

☐ Beachten Sie die allgemeinen Durchführungs-Hinweise auf Seite 25.
☐ Die Verbraucher sind kostenlos und unverzüglich zu unterrichten.

c) Überwachung („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 26.

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 27.

[96] Diese Aussage stammt aus dem Kommentar von Däubler/Wedde/Weichert/Sommer aus Randnummer 5 zu § 30 BDSG, wobei dort ein § 49a BGB genannt wird, den es nicht gibt (vermutlich ist der § 491a BGB gemeint).

10.7 Verweigerung von Auskünften dokumentieren etc. [BDSG_034]

BDSG

In Deutschland kann es gemäß § 34 Abs. 2 BDSG zulässig sein, dass das Recht auf Auskunft (im Sinne des Artikel 15) verweigert wird. Dies muss dokumentiert und gegenüber den betroffenen Personen begründet werden. ACHTUNG: Diese Regelung könnte unionsrechtswidrig sein.

Dieser Pflicht wird das Kürzel **[BDSG_034]** zugeordnet (siehe Seite 14).

10.7.1 Allgemeine Informationen zur Pflicht [BDSG_034]

In der **Fachliteratur** (siehe Seite 518) existiert eine Kommentierung in Kühling/Buchner (2. Auflage).

Hier im § 34 BDSG sollen wohl die Möglichkeiten des Artikel 23 (Beschränkung von Persönlichkeitsrechten) genutzt werden. Allerdings findet sich dort kein Anhaltspunkt, dass bestimmte Aufbewahrungsfristen oder Zwecke eine Beschränkung begründen könnten.

Darf der Verantwortliche gemäß § 34 Abs. 1 Nr. 2 BDSG das Recht auf Auskunft verweigern? Diese Regelung ist möglicherweise **unionsrechtswidrig** (siehe Kühling/Buchner in RdNr. 7-12 zu § 34 BDSG).

10.7.2 Was bedeutet diese Pflicht [BDSG_034] ?

Der deutsche Gesetzgeber will möglicherweise vor allem verhindern, dass sich das Recht auf Datenkopie auch auf Backups und Logfiles bezieht (siehe Plicht **[GVO_015a]** auf Seite 58). Dies bedeutet in der Tat einen hohen Aufwand.

a) Dokumentation der Fälle von Auskunfts-Verweigerung

Der Verantwortliche dokumentiert jedes Szenario, wo er von seinem Recht auf Auskunfts-Verweigerung Gebrauch macht. Dies ermöglicht der Aufsichtsbehörde eine Kontrolle der Sachlage.

b) Begründung gegenüber der betroffenen Person

Wenn eine betroffen Person Auskunft verlangt, so ist die Verweigerung gegenüber der betroffenen Person konkret zu begründen:

- Wurden die Daten nur deshalb gespeichert, weil sie aufgrund gesetzlicher oder satzungsgemäßer Aufbewahrungsvorschriften nicht gelöscht werden dürfen?
- Wurden die Daten ausschließlich zu Zwecken der Datensicherung oder Datenschutzkontrolle gespeichert?
- Inwieweit würde eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern? Hier ist wohl eine Art „Interessenabwägung“ geboten.
- Inwieweit ist eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen?

Selbst diese Auskunft kann verweigert werden, wenn damit die Zwecke der Verweigerung nicht gefährdet werden (beispielsweise die Geltendmachung rechtlicher Ansprüche oder die Verhütung von Schäden durch Straftaten).

c) Strenge Zweckbindung… aber in welchem Kontext?

Der § 34 Abs. 2 Satz 3 BDSG erscheint im Kontext rätselhaft. Der gesamte § 34 BDSG beschreibt die **Verweigerung** von Auskünften. Warum erscheint hier also ein Satz, der sich auf geplante und durchgeführte Auskünfte bezieht?

> *„Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.“*

Die Ähnlichkeit zu § 34 Abs. 5 BDSG-alt ist offensichtlich, aber der Kontext ist ein ganz anderer… den dort geht es eben um die Durchführung von Auskünften (und nicht deren Verweigerung).

10.7.3 Wie erfüllt man diese Pflicht [BDSG_034] ?

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.

[Ab hier eine Lücke aufgrund der Leseprobe...]

10.8 Verarbeitungs-Einschränkung anstelle Löschung kommunizieren [BDSG_035]

BDSG

In Deutschland ist es gemäß § 35 Abs. 2 Satz 2 BDSG zulässig, dass in **nicht automatisierten** Datenverarbeitungen nicht unbedingt gelöscht werden muss. Eine „Einschränkung" der Datenverarbeitung reicht aus. Diese „Einschränkung-statt-Löschung" kann aus verschiedenen Gründen notwendig/zulässig sein. Die betroffene Person soll möglichst darüber unterrichtet werden.

Dieser Pflicht wird das Kürzel **[BDSG_035]** zugeordnet (siehe Seite 14).

10.8.1 Allgemeine Informationen zur Pflicht [BDSG_035]

Die Aufsichtsbehörde kann auf den ersten Blick **keine Geldbuße** verhängen, weil im § 43 BDSG („Bußgeldvorschriften") kein Bezug auf diese Pflicht genommen wird. Doch gemäß Artikel 83 (9) kann der gesamte (Geldbuß-) Artikel 83 analog angewendet werden, wenn eine nationale Rechtsvorschrift keine Geldbußen vorsieht (siehe Seite 577).

In der **Fachliteratur** (siehe Seite 518) existiert eine Kommentierung in Kühling/Buchner (2. Auflage).

!!! Für diese deutsche Regelung gibt es keine offensichtliche Öffnungsklausel (siehe Seite 609). Allenfalls der Artikel 23 käme in Betracht; allerdings sind dessen Voraussetzungen nicht erfüllt (siehe Kühling/Buchner in RdNr. 15-16 zu § 35 BDSG).

10.8.2 Was bedeutet diese Pflicht [BDSG_035] ?

Dieser § 35 BDSG gehört zu den sprachlich ganz besonders schwierigen Bestimmungen. Im Originaltext des Amtsblatts sind die langen Schachtelsätze nicht zu verstehen; insofern ist die entzerrte und mit Markierungen versehene Version auf www.bdsg2018.de/de/35.htm besonders wichtig.

Dieser Paragraf § 35 BDSG trägt die Überschrift „Recht auf Löschung", doch das führt in die Irre. Richtiger wäre „**Einschränkungen** des Rechts auf Löschung".

Das Verständnis des § 35 BDSG ist auch deswegen nicht so einfach, weil er – genau wie Artikel 17 – eine Mischung aus Rechten und Pflichten darstellt. Dies erschließt sich dem Leser aber nach mehrmaligem Lesen.

Die komplexe Sachlage beginnt damit, dass sowohl die Gesetzesbegründung, als auch die bitkom-Stellungnahme nicht darauf eingehen, dass der § 35 Abs. 1 BDSG sich explizit auf „**nicht automatisierte Datenverarbeitungen**" bezieht.
Dieses wichtige Detail übersieht die bitkom am 22.02.2017 mit dem Wortlaut „*Insbesondere in komplexen Datenbanken kann das Löschen einzelner Datensätze oder ihrer Teile die Struktur der Datenbank insgesamt gefährden oder sogar die Datenbank unbrauchbar machen*"); das geht voll am Thema vorbei.

Der Grund für dieses „Missverständnis" liegt wohl darin, dass laut Kühling/Buchner (2. Auflage) diese Einschränkung erst später auf Empfehlung des Innenausschusses hinzugefügt wurde.

Welche „nicht automatisieren Datenverarbeitungen" sind für die nichtöffentlichen Stellen (also die Privatwirtschaft) relevant? Hier drängt sich der § 26 Abs. 7 BDSG auf, der die Beschäftigtendaten auch jenseits automatisierter Verarbeitungen dem Datenschutz unterwirft.

a) Ist der § 35 BDSG unionsrechtskonform?

Das ist eine komplizierte Frage mit komplizierten Antworten. Für diese deutsche Regelung gibt es keine offensichtliche Öffnungsklausel (siehe Seite 609). Allenfalls der Artikel 23 käme in Betracht. Leider muss man jeden Absatz des § 35 BDSG einzeln analysieren:

- § 35 Abs. 1 BDSG
  Die Löschung ist nicht (oder nur mit unverhältnismäßig hohem Aufwand) möglich.
  Insofern sollte der Verantwortliche diese Option vielleicht besser nicht nutzen, denn vor Gericht hätte seine Argumentation eventuell keinen Bestand.

  Darf der Verantwortliche gemäß § 35 Abs. 1 BDSG die Löschung von personenbezogenen Daten unterlassen, falls die Löschung nicht (oder nur mit unverhältnismäßig hohem Aufwand) möglich ist? Diese Regelung ist möglicherweise **unionsrechtswidrig** (siehe Kühling/Buchner in RdNr. 15-16

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 234.

Die GDD hat im Januar 2019 den 133-seitigen Ratgeber „Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG“ veröffentlicht.

11.0.1 Was sind KEINE Pflichten des Datenschutzbeauftragten?

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“*

11.0.2 Begrenzte Haftung des Datenschutzbeauftragten

Welche Haftung muss der Datenschutzbeauftragte gewährleisten?

Die „Zeitschrift für Datenschutz“ 09/2017 sieht auf Seite 411-414 keine wesentlichen Änderungen im Vergleich zum BDSG-alt. Auch die Zeitschrift DuD 03/2018 sieht kein signifikantes Haftungsrisiko. [98]

Die DuD 02/2019 vergleicht DSB-Haftpflichtversicherungen auf Seite 86-89.

Die Aufsichtsbehörde Baden-Württemberg hat im November 2018 den „Praxisratgeber Beauftragter für den Datenschutz Teil II“ veröffentlicht. Dort wird die Verantwortung bzw. das Risiko des Datenschutzbeauftragten ausführlich beschrieben:

> *„DSB sind im Falle der Nichteinhaltung der DS-GVO durch den Verantwortlichen nicht persönlich verantwortlich. […]*
>
> *Die Überwachungspflicht der DSB bewirkt also nicht, dass die DSB im Fall der Nichteinhaltung von Datenschutzvorschriften durch den Verantwortli-*

[98] 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.

[Ab hier eine Lücke aufgrund der Leseprobe...]

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 14).

11.1.1 Allgemeine Informationen zur Pflicht [DSB_001]

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

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 wichtiger Schritt, um die geforderte Unterrichtung in transparenter Form vornehmen zu können (siehe Seite 13).

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 495 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 214 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 165).

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 Pflichten der Beschäftigten (z.B. Auskunftsrechte) und kann die Beschäftigten entsprechend schulen.

e) Unterrichtung des Betriebsrates

Seit dem Betriebsrätemodernisierungsgesetz am 17.06.2021 sind die Datenschutzbeauftragten auch für die Unterrichtung der Betriebsräte zuständig (siehe Seite 17). Insofern sollten auch die Betriebsräte ein Exemplar des PrivazyPlan® erhalten.

11.1.3 Wie erfüllt man diese Pflicht [DSB_001] ?

- ☐ Durch die Aushändigung des PrivazyPlan® ist der Verantwortliche außerordentlich gründlich über seine Pflichten unterrichtet.
- ☐ Alle rechtlichen Neuerungen müssen aufgelistet werden (siehe Seite 495).
- ☐ Sind die Pflichten des PrivazyPlan® noch immer vollständig? Oder sind neue Pflichten hinzugekommen? Dies muss zeitnah kommuniziert werden.
- ☐ Hat sich das Tätigkeitsfeld des Verantwortlichen geändert, sodass neue Rechtsvorschriften zum Tragen kommen? Wenn der Datenschutzbeauftragte dies beurteilen können soll, so muss er durch den Verantwortlichen natürlich vorher entsprechend informiert worden sein.

11.2 Beratung hinsichtlich der Pflichten [DSB_002]

11 Pflichten des DSB

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

Dieser Pflicht wird das Kürzel **[DSB_002]** zugeordnet (siehe Seite 14).

11.2.1 Allgemeine Informationen zur Pflicht [DSB_002]

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

11.2.2 Was bedeutet diese Pflicht [DSB_002] ?

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

a) Beratung des Verantwortlichen

Der Datenschutzbeauftragte muss den Verantwortlichen zu dessen Pflichten beraten.

Der PrivazyPlan® liefert diesbezüglich für jede Pflicht individuelle Vorschläge zum PDCA-Zyklus. Außerdem werden im Kapitel 12 ab Seite 308 zahlreiche Formulare vorgeschlagen.

Wie können die ca. 50 Pflichten priorisiert werden? Dies wird auf Seite 19 ausführlich beschrieben. Der Datenschutzbeauftragte wird hier natürlich gerne beraten.

Die rechtliche Beratung des Datenschutzbeauftragten ist eine Rechtsdienstleistung im Sinne des § 2 Abs. 1 RDG, wie auch der Anwaltsgerichtshof NRW in seinem Urteil Az. 1 AGH 9/19 vom 12.03.2021 entschied.

b) Beratung 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 beraten werden. Dies geschieht beispielsweise über die Beschreibung der Pflicht **[GVO_028a]** und **[GVO_030a]**, wie auf Seite 116 bzw. Seite 214 ausführlich beschrieben.

c) Beratung der Beschäftigten

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

Hier gibt es eine gewisse Parallele zur Pflicht **[GVO_032a]**, wonach der Verantwortliche die Beschäftigten „konkret anzuweisen“ hat (siehe Seite 165).

Diese Beratung findet wohl größtenteils im Tagesgeschäft ab, wenn per E-Mail oder Telefon kommuniziert wird. Darüber hinaus liefert der PrivazyPlan® auch zahlreiche Checklisten, die den Beschäftigten den Umgang mit personenbezogenen Daten erklärt.

e) Beratung des Betriebsrates

Die Betriebsräte sind duch das Betriebsrätemodernisierungsgesetz am 17.06.2021 wohl nicht verpflichtet von den betrieblichen Datenschutzbeauftragten beraten zu werden (siehe Seite 17). Doch die Gesetzesbegründung regt an, dass er besser eine Beratung anfragen sollte.

11.2.3 Wie erfüllt man diese Pflicht [DSB_002]

- ☐ Durch die Aushändigung des PrivazyPlan® ist der Verantwortliche außerordentlich gründlich über seine Pflichten beraten.
- ☐ Bei einer **Datenschutzfolgenabschätzung** (siehe Pflicht **[GVO_035]** auf Seite 182) hat der Verantwortliche gemäß Artikel 35 (2) den Rat des Datenschutzbeauftragten einzuholen.

11.3 Überwachung der Pflichten und Strategien [DSB_003]

Pflichten des DSB

Gemäß Artikel 39 (1b) überwacht der Datenschutzbeauftragte den Verantwortlichen hinsichtlich dessen Einhaltung der Datenschutzvorschriften. Es sind auch die „Strategien“ (z.B. im Sinne des PDCA-Zyklus) überwachen.

Dieser Pflicht wird das Kürzel **[DSB_003]** zugeordnet (siehe Seite 14).

Literatur: • „Die Überwachungsaufgabe des Datenschutzbeauftragten“ auf 88 Seiten inkl. PDF-E-Book für 70 € (bzw. 57 € für GDD-Mitglieder).

11.3.1 Allgemeine Informationen zur Pflicht [DSB_003]

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

11.3.2 Was bedeutet diese Pflicht [DSB_003] ?

Diese Möglichkeit der systematischen Überwachung durch den Datenschutzbeauftragten war ein zentraler Auslöser zur Ausarbeitung des PrivazyPlan®. Dementsprechend wurde der PrivazyPlan® von Anfang an auf diese Überwachungs-Funktion hin konzipiert.

a) Überwachung der Einhaltung der Datenschutzvorschriften

Der Datenschutzbeauftragte überwacht den Verantwortlichen in Hinblick auf dessen Einhaltung der Datenschutzvorschriften.

Der systematische Ansatz des PrivazyPlan® ist in dieser Hinsicht sehr hilfreich.

Jede der ca. 50 Pflichten muss der Datenschutzbeauftragte überwachen. Da das Kalenderjahr ca. 50 Wochen hat, wäre es möglich, dass sich der Datenschutzbeauftragte jede Woche bezüglich einer Pflicht meldet.

Konkrete Überlegungen finden sich in den Folgekapiteln 11.3.3 und 11.3.4.

11.4 Anlaufstelle für Aufsichtsbehörde [DSB_004]

Pflichten des DSB

Gemäß Artikel 39 (1e) dient der Datenschutzbeauftragte für die Aufsichtsbehörde als Anlaufstelle (engl. „contact point“).

Dieser Pflicht wird das Kürzel **[DSB_004]** zugeordnet (siehe Seite 14).

11.4.1 Allgemeine Informationen zur Pflicht [DSB_004]

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

11.4.2 Was bedeutet diese Pflicht [DSB_004] ?

Der Datenschutzbeauftragte als Anlaufstelle ist für die Aufsichtsbehörden sehr wichtig. Für eine schnelle und präzise Klärung von Fachfragen ist den Aufsichtsbehörden an einer kompetenten Person gelegen.

Diese Funktion als „Anlaufstelle“ bedeutet nicht, dass zwangsläufig die gesamte Kommunikation (z.B. per Brief, Telefon oder E-Mail) ausschließlich über den Datenschutzbeauftragten laufen muss. Es muss aber zumindest für den Erstkontakt zur Verfügung stehen.

Das Thema der Kooperation bzw. der Mitwirkung in Hinblick auf die Aufsichtsbehörde gemäß Artikel 31 wird auf Seite 589 beschrieben.

11.4.3 Wie erfüllt man diese Pflicht [DSB_004] ?

Der Datenschutzbeauftragte stellt sicher, dass die Aufsichtsbehörde ihn kontaktieren kann.

In Fällen von längerer Krankheit oder eines längeren Urlaubs sollte eine Vertretung eingeplant werden.

11.5 Anlaufstelle für die betroffenen Personen [DSB_005]

Pflichten des DSB

Gemäß Artikel 38 (4) muss der Datenschutzbeauftragte den betroffenen Personen zur Verfügung stehen, damit diese ihn zu Rate ziehen können.

Dieser Pflicht wird das Kürzel **[DSB_005]** zugeordnet (siehe Seite 14).

11.5.1 Allgemeine Informationen zur Pflicht [DSB_005]

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

11.5.2 Was bedeutet diese Pflicht [DSB_005] ?

Die deutsche Übersetzung geht mit „*zu Rate ziehen*“ wesentlich weiter als der englische Originaltext mit „*to contact*“ oder der französische „*prondre contact*“. Insofern sollte diese Regelung eher als „Anlaufstelle“ interpretiert werden.

Insbesondere hier im Zusammenhang mit den Anliegen der betroffenen Personen ist die Pflicht zur Wahrung der Vertraulichkeit gemäß Artikel 38 (5) von Relevanz.

11.5.3 Wie erfüllt man diese Pflicht [DSB_005] ?

Der Datenschutzbeauftragte stellt sicher, dass eine betroffene Person ihn kontaktieren kann.

In Fällen von längerer Krankheit oder eines längeren Urlaubs sollte eine Vertretung eingeplant werden.

Die Vertraulichkeit von Betroffenen-Anfragen sollte beispielsweise dadurch gewährleistet sein, dass die Details von Tätigkeiten im Rahmen eines eventuell zu erstellenden Jahresberichts ausgeblendet werden.

Wird ein **Berufsgeheimnisträger** gemäß § 203 StGB betreut? Dann ist eine gezielte E-Mail-Kommunikation mit den betroffenen Personen geplant. Das hat zur

Folge, dass erhöhte Anforderungen an den E-Mail-Server des Datenschutzbeauftragten gestellt werden müssen (siehe Seite 435).

11.6 Optionale Pflichten des Datenschutzbeauftragten

Pflichten des DSB

Der Datenschutzbeauftragte kann zusätzliche Pflichten übernehmen, sofern sie nicht zu einem Interessenkonflikt führen.

11.6.1 Verarbeitungsverzeichnis führen

⇧ 11 Pflichten des DSB

Wer kann/soll das Verarbeitungsverzeichnis erstellen und aktuell halten? Die DSGVO trifft weder in Artikel 30, noch im Erwägungsgrund 82 irgendwelche konkrete Aussagen bezüglich der konkreten Zuständigkeit. Die Fachliteratur bezieht (derzeit) durchweg konsequent die Auffassung, dass das Unternehmen mit seinen eigenen Beschäftigten dieses Verarbeitungsverzeichnis auf die Beine zu stellen habe. Nur dann – so die Fachliteratur – könne der Datenschutzbeauftragte völlig konfliktfrei seiner Überwachungspflicht gemäß Artikel 39 (1b) nachkommen.

Doch das Workingpaper „WP 243“ der Artikel-29-Datenschutzgruppe (siehe Seite 599) vertritt eine andere Auffassung:

> „Den Verantwortlichen bzw. den Auftragsverarbeiter hindert somit nichts daran, den DSB die Aufgabe zu übertragen, unter der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters ein Verzeichnis der Verarbeitungsvorgänge [Verarbeitungsverzeichnis] zu führen.“

Auch die Bayerische Aufsichtsbehörde sieht in ihrem Kurzpapier-19 zum Datenschutzbeauftragten keinen Konflikt darin, dass er das Verarbeitungsverzeichnis führt. Auch ein europäischer Datenschützer-Zusammenschluss sieht hier keinen Interessenkonflikt. [99] Dementsprechend kann man sagen: Es ist legitim, wenn der Datenschutzbeauftragte das Verarbeitungsverzeichnis führt.

Doch was genau bedeutet das „Führen“ des Verzeichnisses? Der englische Begriff „to maintain“ kann leider sehr vielfältig übersetzt werden mit „führen“, „unterstützen“, „aufrechterhalten“, „nachpflegen“.
Was ist also gemeint? Das Festlegen der zu dokumentierenden Inhalte? Die Fachabteilungen zu sensibilisieren? Die Details der Verarbeitung in Erfahrung bringen? Das Abklären aller relevanten Details? Die Beurteilung, ob alles vollständig und rechtmäßig ist? Das Speichern in einer Software? Die Meldung des Ergebnisses an die Fachabteilungen? Die regelmäßige Nachkontrolle? Die Information an die Geschäftsführung, wenn es Probleme gibt? … es gibt also viele wichtige Details, die sich hinter dem simplen Begriff „Verarbeitungsverzeichnis führen“ verbergen können.

Angesichts dieser vielen Fragen muss das Unternehmen zunächst eine entsprechende Strategie entwickeln und sie dann in die Praxis umsetzen.

11.6.2 Mitarbeiter schulen

⇧ 11 Pflichten des DSB

Es gibt verschiedene Interpretationen bezüglich des Artikel 39 (1b): Soll der Datenschutzbeauftragte die Mitarbeiterschulung selbst durchführen, oder soll er nur die Durchführung überwachen?

Vermutlich ist hier ein Kompromiss sinnvoll: Der Verantwortliche entscheidet darüber, welche Mitarbeiter wie oft geschult werden… und der Datenschutzbeauftragte führt die Schulung aus.

Die Schulung passt thematisch gut zur Pflicht **[GVO_032a]** auf Seite 165.

[Ab hier eine Lücke aufgrund der Leseprobe...]

[99] Die CEDPO hat in einem Brief am 07.10.2016 darauf hingewiesen:
„*The GDPR provides that the record must be maintained by the data controller or by its representative (art 30). The DPO may then be charged to maintain the record as a controller's representative. This shall not be considered as a conflict of interest*“. Aus Sicht der Datenschützer-Verbände ist es also kein Interessenkonflikt, wenn der DSB das Verarbeitungsverzeichnis (weiter-) pflegt.

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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 Belangen 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

Basis-Checklisten

Wir schlagen vor, Sie beginnen die ersten 2-3 Stunden mit ausführlicher Lektüre:[100]

⚠ Drucken Sie die folgenden Seiten des Anhangs aus:

- die Liste der Verarbeitungsbeispiele ab Seite 404
- die Kurzzusammenfassung aller Pflichten ab Seite 674
- das ausführliche Inhaltsverzeichnis ab Seite 686
- die tabellarische Übersicht aller Pflichten ab Seite 689
- den Index ab Seite 700

… 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.gvo2018.de bzw. 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 609. 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 502 ausführlich beschrieben wird.

☐ Lesen Sie die **Kurzzusammenfassung aller Pflichten** ab Seite 674 (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 518), 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 518.

12.1.2 Personelle Entscheidungen treffen und mit den Arbeiten beginnen

Basis-Checklisten

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 „Ein grober Plan zur Umsetzung der DS-GVO“ ab Seite 19 werden die Haupt-Akteure konkret genannt:

[Ab hier eine Lücke aufgrund der Leseprobe...]

[100] Der folgende blaue Kasten ist ein Querverweis auf die „Originalstelle“ auf Seite 10. Von dort aus gelangen Sie dann auf die gewünschten Seiten.

12.2 Nachweis der Einhaltung der Grundsätze [GVO_005]

Formulare

Gemäß Artikel 5 (2) unterliegt der Verantwortliche einer generellen „*Rechenschaftspflicht*“ (engl. „Accountability“). 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.

➔ Siehe Pflicht **[GVO_005]** auf Seite 102.
➔ Siehe Pflicht **[AUX_008]** auf Seite 323.

12.2.1 Datenschutz-Leitlinie der Geschäftsführung

Nachweis der Einhaltung der Grundsätze

Das Fundament des Datenschutzes wird von der Geschäftsführung gelegt. Die folgende Selbstverpflichtung zeigt exemplarisch, wie solch ein Dokument aussehen kann. Idealerweise wird die Leitlinie von der Geschäftsführung persönlich unterschrieben und im Unternehmen bekannt gemacht.

Hier im PrivazyPlan® wird das Wort „**Leitlinie**“ (engl. „guideline“) im Sinne einer groben Richtschnur verwendet. Andere Autoren verwenden auch schon mal den Begriff „Richtlinie“ (engl. „Policy“), der aber eigentlich sehr viel verbindlicher und praxisnäher zu verstehen ist.

Siehe auch **VdS-Richtlinie 10010** (Seite 512) im dortigen Kapitel 5 („Leitlinie zum Datenschutz“). Auf Wunsch stellen wir Ihnen eine entsprechende Leitlinie mit 15 Seiten Umfang exemplarisch zur Verfügung.

Falls das Mini-Datenschutz-Managementsystem genutzt wird (siehe Seite 29), so kann die Datenschutz-Leitlinie beispielsweise in der vorbereiteten Verzeichnisstruktur im Unterverzeichnis \GVO_005\ abgelegt werden („Datenschutz-Managementsystem einrichten“).

Hier in der Leitlinie können Sie auch die Ergebnisse der allgemeinen Überlegungen publizieren (siehe Seite 16).

Der Datenschutz-Berater 01/2022 liefert auf Seite 18-21 viele gute inhaltliche Anregungen für eine Leitlinie. Dort wird auch thematisiert, wie man solch **eine Leitlinie rechtlich korrekt verankert**, damit sie auch vor Gericht wirksam ist (nämlich die Beschäftigten verpflichtet und das Topmanagement entlastet). Konkret wird vorgeschlagen, dass die Beschäftigten den Erhalt der Leitlinie im Sinne des § 368 BGB aktiv quittieren. Der Autor des Fachartikels rät gut begründet davon ab eine Formulierung wie *„hiermit bestätige ich die Policy gelesen zu haben und damit einverstanden zu sein“* zu nutzen.

In der Fachliteratur gibt es weitere Beispiele für eine solche Leitlinie: • Die GDD-Praxishilfe DS-GVO VIII („Unternehmensrichtlinie zur Datenschutz-Organisation“) • im Fachbuch „Datenschutz-Compliance nach der DS-GVO“ wird auf Seite 36 auf solch eine Leitlinie eingegangen. Insgesamt liefert das Buch 43 Treffer zu diesem Stichwort.

DATENSCHUTZ-LEITLINIE der Mustermann GmbH

UNVERBINDLICHER ENTWURF

Diese Datenschutz-Leitlinie bringt zum Ausdruck, wie die Geschäftsführung mit den **personenbezogenen Daten** von Beschäftigten, Kunden, Lieferanten etc. umgehen will.

EINFÜHRUNG

Datenschutz betrifft uns alle. Wir alle stellen unsere persönlichen Daten verschiedensten Unternehmen oder Diensten zur Verfügung. Wir alle gehen davon aus, dass unsere Daten sorgsam behandelt und geschützt werden.

Genau dies fordern auch unsere Beschäftigten, Kunden und Lieferanten.

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.3 Rechtsgrundlage von Verarbeitungen [GVO_006 etc.]

Formulare

12.3.1 Interessenabwägung durchführen [GVO_006]

Formulare „Rechtsgrundlage von Verarbeitungen“

An sechs Stellen in der DS-GVO (und fünf Stellen im BDSG) wird von **„überwiegenden“ Interessen** gesprochen. An jenen Stellen muss der Verantwortliche abwägen, ob die schützenswerten Interessen der betroffenen Personen seine betrieblichen Interessen überwiegen.

Unter der Überschrift „Interessenabwägung“ ist diese Art der Überlegung in Deutschland seit vielen Jahren bekannt. Die besondere Schwierigkeit liegt darin, dass materielle Interessen des Verantwortlichen mit **im**materiellen Interessen der betroffenen Personen abgewogen werden müssen. Doch leider werden hier „Äpfel mit Birnen verglichen“. Wie soll man dies auf eine objektive Weise vornehmen? Die Fachwelt schweigt sich hierüber komplett aus. [104]
Die ZD 11/2018 berichtet auf Seite 514-520 über das sogenannte „**3x5-Modell**“; hierbei werden 15 Kriterien zur Beurteilung der Risiken aus Sicht der betroffenen Personen aufgestellt. Doch auch hier gilt: Die eigentliche Abwägung bleibt immer noch „subjektiv“.

[104] Im September 2019 gab es eine interessante Fragestellung: Dürfen die Telefonnummern von Mietern an Handwerker weitgegeben werden, um Schadensreparaturen schnell zu organisieren? Zwei Aufsichtsbehörden kommen zu gegensätzlichen Ergebnissen (in beiden Fällen leider nicht konkret begründet). Auch in gerichtlichen Entscheidungen erfährt der Leser nur das Ergebnis einer Interessenabwägung; die genaue Herleitung bleibt unbekannt. Siehe auch hier.

Im Streitfall wird eine betroffene Person (bzw. eine Aufsichtsbehörde) aber den Nachweis einer Interessenabwägung fordern. Wenn der Verantwortliche diesen nicht (schriftlich) **nachweisen** kann, dann geht dies zu dessen Lasten.

Die folgenden Anlässe für eine Interessenabwägung werden in dem unten folgenden Formular NICHT berücksichtigt, weil sie eher selten erforderlich sind:
(a) Artikel 18 (1d) zur Einschränkung der Verarbeitung, **(b)** Artikel 21 (1) zum Widerspruch gegen berechtige Interessen des Verantwortlichen, **(c)** Artikel 49 (1) mit Erwägungsgrund 113 für Einzelfälle von Drittland-Übermittlungen, **(d)** § 24 BDSG zur Weiterverarbeitung zu anderen Zwecken, **(e)** § 27 BDSG zu wissenschaftlichen Zwecken, **(f)** § 29 BDSG zur Geheimhaltung von Verarbeitung, **(g)** § 32 BDSG zur Geheimhaltung von Daten-Erhebung.

[Im Rahmen von PrivazyPlan® wird das Dossier „Interessenabwägung“ 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.]

\PrivazyPlan\GVO_006
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Interessenabwägung einer neuen (Daten-) Verarbeitung

\PrivazyPlan\GVO_006\Interessenabwägung\Theorie.pdf
… dort finden Sie alle Aspekte einer objektiven Interessenabwägung. Bitte lesen Sie dies als fachliche Vorbereitung.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

In Bezug auf die Verarbeitung mit dem Namen: .....

ist in Hinblick auf die Rechtsgrundlage des „berechtigten Interesses“ gemäß Artikel 6 (1f) eine Interessenabwägung erforderlich.

Die Wahl dieser Rechtsgrundlage hat ihren Preis: Die geplante (Daten-) Verarbeitung muss penibel dahingehend optimiert werden, dass die Rechte und Freiheiten der betroffenen Personen so wenig wie möglich beeinträchtigt werden. Es darf also keine milderen Mittel geben, um die Ziele zu erreichen. Sie müssen die tatsächliche Erforderlichkeit nachweisen können. Sie müssen aktiv und objektiv nach möglichen Gegeninteressen der betroffenen Personen suchen, die mög-

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.4 Einwilligungstexte planen und formulieren [GVO_007 etc.]

Formulare

12.4.1 Planung von Einwilligungen

Einwilligungstexte planen und formulieren

Die DS-GVO formuliert viele Pflichten hinsichtlich der Einwilligung. Die folgende Checkliste liefert einen ersten Anhaltspunkt darüber, was alles zu beachten ist.

➔ Dieses Formular betrifft viele verschiedene Pflichten (siehe unten).

Das unten folgende Statusblatt ist ein guter Ansatz, um die Forderung der Artikel-29-Datenschutzgruppe auf Seite 20 des „WP 259“ zu erfüllen: „*The controller could retain a documentation of* ***consent workflow***“. Dieses Workingpaper „WP 259“ hat in vielerlei Hinsicht umfassende Forderungen zur Einwilligung.

\PrivazyPlan\GVO_007
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Im Folgenden finden Sie einen beispielhaften Ansatz für ein konkretes Formular.

Statusblatt für die Planung einer neuen Einwilligung

Eine neue Einwilligung ist geplant.

☐ Es geht um diesen Sachverhalt: .....

☐ Die Einwilligung hat das Kürzel: .....(z.B. „e001“, siehe Seite 28)

☐ Dieser Vorgang wird durch den Datenschutzbeauftragten unterstützt?
☐ ja / ☐ nein: ..

☐ Der Einwilligungstext lautet: „.....“

a) Planung einer Einwilligung

Bevor eine Einwilligung konkret formuliert wird, sollte der Verantwortliche zumindest die folgenden Aspekte kurz prüfen:

☐ Ist wirklich die **Notwendigkeit** einer Einwilligung als Rechtsgrundlage gegeben? Es gibt keine Gesetze oder Verträge oder berechtigten Geschäftsinteressen, die diese Datenverarbeitung legitimieren könnten? Dann müssen Einwilligungen eingeholt werden und in Kauf genommen werden, dass die Einwilligung von den Personen entweder verweigert oder nachträglich widerrufen werden könnten. Siehe Pflicht **[GVO_006]** im Kapitel 4.1 auf Seite 130 (dort in Fußnote 36 wird über ein Bußgeld wegen irrtümlich angewendeter Einwilligungen berichtet).

☐ Welche **Fachabteilungen** (und ggf. auch der Datenschutzbeauftragte) sollen bei der Genehmigung neuer Einwilligungstexte einbezogen werden?

☐ Jede von einer betroffenen Person erteilte Einwilligung sollte dauerhaft dokumentiert werden, um im Zweifelsfall jederzeit als Beweismittel dienen zu können. Wann wurde die Einwilligung erteilt? Was genau war der Wortlaut? Siehe Pflicht **[GVO_007]** im Kapitel 4.3 auf Seite 142. Wie stellen Sie das sicher?

O Auf **Websites** kann z.B. die Tracking-Einwilligung durch ein spezielles Cookie gespeichert werden (siehe Seite 633). Dokumentieren Sie die Vorgehensweise ganz präzise und erstellen Sie eine Kopie des Sourcecodes (z.B. JavaScripts), um jederzeit lückenlos nachweisen zu können, dass Sie wirksame Einwilligungen eingeholt haben.
Werden Cookies durch **Drittland-Anbieter** genutzt (z.B. aus den USA)? Dann spielt der Drittland-Aspekt eine wichtige Rolle. Falls Sie hier bereits einen Einwilligungstext implementiert haben, so sollte dieser um den Drittland-Aspekt erweitert werden (siehe weiter unten).

☐ Die erteilte Einwilligung muss jederzeit und einfach **widerrufbar** sein. Auch der erfolgte Widerruf muss dauerhaft dokumentiert werden. Siehe Pflicht **[GVO_007b]** im Kapitel 4.5 auf Seite 148. Wie stellen Sie das sicher?

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.5 Dritt-Erhebung der betroffenen Person melden [GVO_014]

Formulare

Gemäß Artikel 14 (1) und Artikel 14 (2) muss der Verantwortliche die betroffenen Personen darüber informieren, dass ihre Daten an anderer Stelle (also durch einen Dritten) erhoben wurden. Dies geschieht spätestens innerhalb von vier Wochen. Doch es gibt auch zahlreiche Ausnahmen.

➔ Siehe Pflicht **[GVO_014]** auf Seite 50.

Im Folgenden finden Sie einen beispielhaften Ansatz für ein konkretes Formular. Sie könnten es anpassen und speichern unter:
`\PrivazyPlan\GVO_014\GVO_014_Checkliste.docx`

Information über Dritt-Erhebung

Bezüglich der Person (Nachname, Vorname) ……

wurden im Rahmen der Verarbeitung „……“

Daten durch den Dritten …… erhoben.

Eine Information ist (gemäß der Liste auf Seite 51) **erforderlich**, weil
- ☐ die betroffene Person davon keine Kenntnis hatte
- ☐ die Informationserteilung problemlos möglich ist
- ☐ kein unverhältnismäßig hoher Aufwand besteht
- ☐ es sich nicht um einen „privilegierten Zweck“ handelt (Archiv, Forschung, Statistik)
- ☐ es keine berechtigte Geheimhaltungsinteressen gibt
- ☐ keine Rechtsvorschrift dies gebietet und geeignete Schutzmaßnahmen vorgesehen sind
- ☐ keine berufliche Schweigepflicht besteht

Wenn die Informations-Erteilung notwendig ist: Wieviel Zeit haben Sie dafür:

- ☐ Sie muss **sofort** erfolgen, weil der Zweck der Verarbeitung (u.a.) darin besteht, dass die Daten einem Dritten übermittelt werden. [Die Offenlegung durch eine Auftragsverarbeitung wird nicht weiter betrachtet, weil diese von Brüssel wohl nicht gemeint war.]
- ☐ Sie muss **sofort** mit der ersten Kontaktaufnahme erfolgen, die auch tatsächlich konkret vorgesehen ist.
- ☐ Es gibt keine besonderen Erfordernisse, wir haben **vier Wochen** Zeit.

☐ Besorgen Sie sich den für diese Verarbeitung relevanten Informationstext. Möglicherweise steht ein allgemeiner Transparenz-Texte zur Verfügung (siehe Kapitel 12.15.5 Seite 415).

☐ Die Information wurde erteilt:

Am folgenden Tag: …

Auf dem folgenden Weg: ☐ Post ☐ Telefon ☐ ~~Fax~~ ☐ E-Mail ☐ Sonstiges: ….

Die erteilte Information wird (z.B. für drei Jahre) archiviert?

- ☐ ja
- ☐ nein

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.6 Auskunft erteilen an betroffene Person [GVO_015]

Formulare

Das Recht auf Auskunft gemäß Artikel 15 (1) und Artikel 15 (2) ist sehr weitreichend. Die betroffenen Personen (bzw. Bevollmächtigte, wie z.B. Erben) müssen einen entsprechenden Antrag stellen. Es müssen **keine Details** beauskunftet werden. Diese Pflicht ist ernst zu nehmen, weil fehlende oder grob unvollständige Auskünfte von Jedermann leicht festzustellen sind.

➔ Siehe Pflicht [GVO_015] auf Seite 55.

Die hier vorliegende Checkliste regelt die Vorgehensweise für den Fall, dass die betroffene Person die Auskunft nicht eigenständig (auf elektronischem Wege) einholen konnte.

\PrivazyPlan\GVO_015a
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Auskunft erteilen an betroffene Person

Bezüglich der Person (Nachname, Vorname) ……

☐ Das **Formular „Persönlichkeitsrechte erfüllen“** im Kapitel 12.1.5 des PrivazyPlan® wurde berücksichtigt. Dort finden sich viele wichtige Prüfungen, bevor/nachdem das konkrete Verlangen der betroffenen Person erfüllt wird. Insbesondere die korrekte Identifizierung spielt eine große Rolle.

Die Auskunft wurde erteilt:

Datum: …

Auf dem folgenden Weg:
☐ Post ☐ Telefon ~~☐ Fax~~ ☐ E-Mail ☐ Sonstiges: ….

☐ Besorgen Sie sich den für diese Verarbeitung relevanten Auskunftstext. Möglicherweise steht ein allgemeiner Transparenz-Texte zur Verfügung (siehe Kapitel 12.15.5 Seite 415).

Die erteilte Information wird (z.B. für drei Jahre) archiviert?
☐ ja
☐ nein

a) Ausnahmeregelungen für Deutschland

Im BDSG (in der Fassung ab dem 25.05.2018) existieren zahlreiche Ausnahmen von der Auskunft-Pflicht. [108] Bevor Sie diese Ausnahmeregelung anwenden: Prüfen Sie, ob die Geschäftsführung möglicherweise geplant hat, dass diese Regelung nur in absoluten Ausnahmefällen angewendet werden soll.

Prinzipiell haben die betroffenen **kein Recht auf Auskunft**, wenn

entweder

☐ Es sich um wissenschaftliche oder historische Forschung handelt (§ 27 Abs. 2 BDSG), oder
☐ die Daten in Archiven gespeichert sind und dem öffentlichen Interesse dienen (§ 28 Abs. 2 BDSG), oder
☐ Gründe der Geheimhaltung bzw. berechtigte Interessen Dritter dagegensprechen (§ 29 Abs. 1 Satz 2 BDSG), oder
☐ auch keine Informationspflicht bestünde, sofern in Rahmen von § 33 Abs. 1 Nr. 2 b BDSG eine zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden würde (§ 34 Abs. 1 Nr. 1 BDSG).

[Ab hier eine Lücke aufgrund der Leseprobe...]

[108] Der hier aufgeführte Katalog an Kriterien ist wieder einmal einzigartig komplex. Der Autor des PrivazyPlan® hat sich alle Mühe gegeben die verzwickten Verweise des BDSG übersichtlich darzustellen. Einmal mehr fragt sich der Rechtsanwender, ob der deutsche Gesetzgeber sich überhaupt die Mühe gemacht hat, das eigene Gesetz mit Sinn und Verstand zu lesen.

12.7 Datenkopie aushändigen an die betroffene Person [GVO_015a]

Formulare

Das Recht auf Datenkopien gemäß Artikel 15 (3) und Artikel 15 (4) gibt den Betroffenen ein (fast) uneingeschränktes Recht auf Kopien ihrer Daten. Gemäß Erwägungsgrund 63 kann der Verantwortliche um eine Präzisierung bitten (um nicht immer ALLE Daten kopieren zu müssen); doch die betroffene Person kann trotzdem ALLE Daten einfordern.

➔ Siehe Pflicht **[GVO_015a]** auf Seite 58.

12.7.1 Leitfaden für die Fachabteilungen

Die Zurverfügungstellung von Datenkopien im Sinne der Pflicht **[GVO_015a]** ist wahrlich keine triviale Angelegenheit; die vielen offenen Fragen ab Seite 58 zeigen deutlich, dass es viele Fallstricke gibt. Aus diesem Grund benötigen die Kolleginnen und Kollegen in den Fachabteilungen einen konkreten Leitfaden. Nur so können Diskussionen, Fehler und Widersprüche vermieden werden.

Übrigens kann das folgende Dokument ebenfalls zur Erfüllung der Pflicht **[GVO_020]** zur **Daten-Übertragbarkeit** verwendet werden (siehe Seite 88). Es müssten zwar einige inhaltliche Änderungen vorgenommen werden, aber das Prinzip ist sehr ähnlich.

Leitfaden für die Erstellung von Datenkopien

[Dieser Leitfaden ist nur ein unverbindliches Beispiel und sollte nicht unreflektiert übernommen werden.]

Liebe Kolleginnen und Kollegen,

die seit dem 25.05.2018 geltende EU Datenschutz-Grundverordnung (DS-GVO) gibt den betroffenen Personen im Artikel 15 (3) ein Recht auf **Datenkopie**. Demzufolge müssen wir (prinzipiell) alle von uns gespeicherten Daten offenlegen.

Sie erhalten diesen Leitfaden, weil Ihr Name im Verarbeitungsverzeichnis als fachliche Kontaktperson für ein oder mehrere Verarbeitungen genannt ist.

Jedes Verlangen auf Datenkopie ist ein kritischer Vorgang. Die betroffene Person wird diesen Vorgang meist nicht aus Langeweile anstoßen. Vielmehr ist zu befürchten, dass dies nur die Vorstufe für den „eigentlichen“ Konflikt darstellt (Gerichtsprozess, Beschwerde bei der Aufsichtsbehörde, Schadenersatz-Forderungen, … siehe Seite 575). Insofern ist Schnelligkeit und Präzision von hoher Wichtigkeit.

a) Die generelle Vorgehensweise

Prinzipiell gehen wir folgendermaßen vor:

1.) Der Datenschutz-Koordinator übernimmt die **Projekt-Organisation** und legt ein Projekt-Codewort fest (z.B. „*Monsun*“). Alle Fachabteilungen (und betroffenen Auftragsverarbeiter) erhalten das Codewort und den Wortlaut des Datenkopie-Verlangens (u.a. mit dem Namen und ggf. einer Kundennummer der betroffenen Person).
Außerdem erhält die Fachabteilung eine Liste der Verarbeitungen, für die eine Datenkopie in Frage käme (an dieser Stelle zahlt sich ein gutes Verarbeitungsverzeichnis aus, siehe Kapitel 3.3 im PrivazyPlan®).

2.) Jede **Fachabteilung** zippt die Datenkopie-Dateien mit einem eigenen Passwort; idealerweise im „ZIP-Crypto“-Format mit einem 16-stelligen Passwort hoher Güte (das Passwort sollte drei Jahre lang archiviert werden – auf Papier oder elektronisch).
Der jeweilige ZIP-Datei-Name könnte lauten: „*2019 01 31 V_123 Personalakte Erwin Müller MONSUN.zip*“ (und sollte somit auch den Namen und ggf. das Kürzel der zugrundeliegenden Verarbeitung enthalten).
Falls die Fachabteilung über KEINE Daten verfügt, so kann dies in einem simplen Textdokument kurz festgestellt werden („Über Sie wird keine Personalakte geführt.“); nur auf diese Weise kann verbindlich dokumentiert werden, dass trotz der Suche keine Daten gefunden wurden.

3.) Der Datenschutz-Koordinator **sammelt** alle diese verschlüsselten ZIP-Dateien, um sie dann der betroffenen Person z.B. per E-Mail auszuhändigen. Dieser Datenbestand sollte für drei Jahre archiviert werden (bis die Verjährung eintritt).

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.8 Berichtigung von Daten durchführen [GVO_016]

Formulare

Gemäß Artikel 16 haben betroffene Personen das Recht auf eine Berichtigung von unrichtigen Daten. In der Datenverarbeitung ist ein Datenfeld aufzunehmen, wo die betroffene Person eine „ergänzende Erklärung“ hinterlegen kann (um den Kontext korrekt und unmissverständlich klarzustellen).

➔ Siehe Pflicht **[GVO_016]** auf Seite 70.

Die hier vorliegende Checkliste regelt die Vorgehensweise für den Fall, dass die betroffene Person die Berichtigung nicht eigenständig (auf elektronischem Wege) vornehmen konnte.

\PrivazyPlan\GVO_016
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Berichtung durch betroffene Person

Name der betroffenen Person: …

Das Berichtigungs-Verlangen wurde vorgetragen am …
per ☐ Post ☐ E-Mail ☐ Sonstiges: …

☐ Das **Formular „Persönlichkeitsrechte erfüllen“** im Kapitel 12.1.5 des PrivazyPlan® wurde berücksichtigt. Dort finden sich viele wichtige Prüfungen, bevor/nachdem das konkrete Verlangen der betroffenen Person erfüllt wird. Insbesondere die korrekte Identifizierung spielt eine große Rolle.

Dieses Verlangen wird zunächst dokumentiert ☐ auf Papier ☐ in einem Ticket-System [ID= …….]

Die folgenden Daten sollen berichtigt werden: …

Das Verlangen ist ☐ berechtigt / ☐ unberechtigt, weil: …

Betroffen sind die folgenden Verarbeitungen: …

Die Berichtigung wurde vorgenommen von … am …

☐ Eine mögliche Berichtigung in den **Backups** (siehe Seite 365) wurde geprüft:
- ☐ Es gibt keine Backups und daher muss nichts berichtigt werden. [110]
- ☐ Auch die Daten in den Backups werden berichtigt: …
- ☐ Keine Berichtigung, aber Vermerke für den Fall der Widerherstellung: …
- ☐ Sonstiges: …

Den folgenden externen Empfänger wurde die Berichtigung gemäß Artikel 19 (bzw. Pflicht **[GVO_019]** im Kapitel 2.11)

☐ mitgeteilt, weil …

☐ **nicht** mitgeteilt, weil dies
- ☐ unmöglich ist: ..
- ☐ unverhältnismäßig ist: …

[110] Fehlende Backups sind nicht immer ein Problem. Insbesondere bei Auftragsverarbeitern kann manchmal auf Backups verzichtet werden, weil der Verantwortliche die Daten jederzeit wieder liefern könnte, falls sie beim Auftragsverarbeiter verloren gingen. Insofern können fehlende Backups eine geeignete Maßnahme zur Datenminimierung gemäß Artikel 25 sein; siehe Pflicht **[GVO_025]** auf Seite 102.

12.9 Löschen… [GVO_017], [GVO_017a]

Formulare

Das Löschen ist ein Verarbeitungsschritt gemäß Artikel 4 Nr. 2.

12.9.1 Löschkonzept [GVO_017]

Löschen…

Im Artikel 17 (1) werden verschiedene betriebliche Gründe und Umstände für das Löschen von Daten beschrieben. Das Unternehmen muss demnach selbst laufend prüfen, ob es die Daten noch speichern darf, oder ob es diese unverzüglich löschen muss. Ein „versehentliches Liegenlassen“ von personenbezogenen Daten kann mit Geldbußen geahndet werden.

➔ Siehe Pflicht [GVO_017] auf Seite 72.
➔ Siehe die „weiche“ Pflicht [AUX_010] auf Seite 324 zum Löschkonzept.
➔ Siehe konkrete Löschfristen auf Seite 550.

In der Fachliteratur (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Datenschutz-PRAXIS 05/2019 Seite 7-10 ● Datenschutz-PRAXIS 12/2018 Seite 8-11 ● DatenschutzPraxis 08/2017 Seite 13-14 ● DatenschutzPraxis 04/2016 Seite 9-12 mit einer Schritt-Für-Schritt-Anleitung ● DuD 08/2016 Seite 528-533. ● DIN-Leitlinie für Löschkonzept.

Die DIN 66398 schreibt in der Einleitung: „*Um eine rechtskonforme Löschung von personenbezogenen Daten sicherzustellen, ist es für die verantwortliche Stelle unabdingbar, ein Regelwerk zu entwickeln und Verantwortung zuzuweisen. Die Etablierung eines solchen Löschkonzepts ist eine komplexe und umfangreiche Aufgabe*“.

\PrivazyPlan\GVO_017
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Löschkonzept

Löschkonzept für das Unternehmen: .....

Beachten Sie die Planungsschritte der Pflicht [GVO_017] im Kapitel 2.7 auf Seite 73 !

1.) Identifizieren der Verarbeitungen

Welche Daten müssen gelöscht werden, wenn deren Zweck erfüllt ist, und eine Speicherung nicht mehr erforderlich ist? Diese Frage beantwortet das Verarbeitungsverzeichnis.

☐ Besorgen Sie sich das Verarbeitungsverzeichnis (gemäß Artikel 30 und der Pflicht [GVO_030] im Kapitel 3.3 auf Seite 110). Die Liste liegt entweder bei Ihrem Datenschutzbeauftragten oder bei einer anderen dafür zuständigen Person. Anhand dieser Liste sehen Sie die Aufbewahrungs- bzw. Löschfrist aller Datenkategorien einer jeden Verarbeitung.
Sollte das Verarbeitungsverzeichnis noch nicht komplett sein, so holen Sie dies schnell nach.

Für die unten folgenden Aufgaben müssen die folgenden Informationen im Verarbeitungsverzeichnis enthalten sein:

- Name der Verarbeitung,
- Zweck der Verarbeitung,
- Rechtsgrundlage der Verarbeitung,
- Welche Daten werden gespeichert (Datenkategorien und -Details)
- Der Ort der Speicherung im Sinne von
  (a) eigene Computer und Akten
  (b) Auftragsverarbeiter (Pflicht [GVO_028] im Kapitel 7.3 auf Seite 207)
  (c) gemeinsam Verantwortliche (Pflicht [GVO_026] im Kapitel 7.1 auf Seite 192)

Somit ist im ersten Schritt geklärt, welche Daten sich wo befinden.

2.) Festlegung der Löschfristen

Legen Sie für jede Verarbeitung fest, wann der Zweck der Verarbeitung erfüllt ist. Möglicherweise gibt es gesetzliche Aufbewahrungsfristen zu beachten.

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.10 Einschränkung der Verarbeitung durchführen [GVO_018]

Formulare

Gemäß Artikel 18 (1) können betroffene Personen unter bestimmten Umständen eine „Einschränkung der Verarbeitung“ verlangen; oftmals wird dies auch als „Sperrung“ bezeichnet. Der Sinn dieser „Einschränkung“ liegt darin, dass in verschiedenen Streitfällen die Daten erst einmal „eingefroren“ werden, bis eine Klärung der Sachlage erfolgt ist.

➔ Siehe Pflicht **[GVO_018]** auf Seite 80.

➔ Siehe Pflicht **[BDSG_035]** auf Seite 288 bezüglich der Unterrichtung über eine „Einschränkung der Verarbeitung“ statt Löschung.

\PrivazyPlan\GVO_018
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Einschränkung der Verarbeitung

Es gibt hier **zwei** komplett verschiedene Szenarien:
a) Die betroffene Person verlangt die Einschränkung der Verarbeitung
b) Das Unternehmen schützt die Interessen der betroffenen Person

a) Die betroffene Person verlangt die Einschränkung der Verarbeitung

Die betroffene Person (Nachname, Vorname): ……

verlangt die Einschränkung der Verarbeitung

am: …

per ☐ Telefon ☐ Brief ☐ E-Mail ☐ Sonstiges: …

☐ Das **Formular „Persönlichkeitsrechte erfüllen“** im Kapitel 12.1.5 des PrivazyPlan® wurde berücksichtigt. Dort finden sich viele wichtige Prüfungen, bevor/nachdem das konkrete Verlangen der betroffenen Person erfüllt wird. Insbesondere die korrekte Identifizierung spielt eine große Rolle.

Betroffen sind diese Verarbeitungen: …

Der gewünschte Zeitraum beträgt: ☐ unendlich ☐ für ……. Tage ☐ Sonstiges: ….

Dieses Verlangen wird zunächst dokumentiert ☐ auf Papier ☐ in einem Ticket-System [ID= ……]

Begründung der betroffenen Person (siehe Kapitel 2.10.2 Seite 80):

☐ Die Richtigkeit der Daten wird bestritten: [113] …

☐ Die Verarbeitung ist nicht rechtmäßig: …

☐ Löschung soll unterbleiben, damit die betroffene Person Rechtsansprüche ausüben kann

☐ Die betroffene Person hat ihr **Widerspruchsrecht** gemäß Artikel 21 wahrgenommen (siehe Formular im Kapitel 12.12 auf Seite 372), doch sollen die Daten nicht gemäß Artikel 17 (1c) gelöscht werden. Eine besondere Begründung für dieses Verlangen ist nicht notwendig.

Dieses Verlangen ist

☐ rechtmäßig ☐ nicht rechtmäßig, weil …

Die Einschränkung der Verarbeitung wurde vorgenommen:

☐ ja ☐ nein, weil…

[Ab hier eine Lücke aufgrund der Leseprobe...]

[113] Es bedarf **qualifizierter Gründe** seitens der betroffenen Person. Ohne stichhaltige Gründe ist eine Einschränkung der Verarbeitung nicht geboten. Siehe Beschluss des VG Stade (Az. 1 B 1918/18 vom 09.10.2018) in RdNr. 33.

12.11 Recht auf Datenübertragbarkeit ermöglichen [GVO_020]

Formulare

Betroffene Personen haben gemäß Artikel 20 das Recht, dass die von ihnen bereitgestellten Daten exportiert (und zu einem Konkurrenz-Anbieter übertragen) werden können. Dies betrifft nur die automatisierten Verarbeitungen, die auf einem Vertragsverhältnis oder einer Einwilligung beruhen. Dieses Recht darf nicht verwechselt werden mit dem „Recht auf Kopie“ gemäß Artikel 15 (3) (siehe Seite 70).

➔ Siehe Pflicht [GVO_020] auf Seite 88.

Die hier vorliegende Checkliste regelt die Vorgehensweise für den Fall, dass die betroffene Person die Datenübertragung nicht eigenständig (auf elektronischem Wege) vornehmen konnte.

Im Folgenden finden Sie einen beispielhaften Ansatz für ein konkretes Formular.

\PrivazyPlan\GVO_020
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Recht auf Datenübertragbarkeit ermöglichen

⚠ Die Aushändigung einer Datenkopie an die betroffene Person ist mit einer Vielzahl an **Risiken** verbunden (siehe Seite 66).

Betroffene Person (Nachname, Vorname) ……

☐ Das **Formular „Persönlichkeitsrechte erfüllen“** im Kapitel 12.1.5 des PrivazyPlan® wurde berücksichtigt. Dort finden sich viele wichtige Prüfungen, bevor/nachdem das konkrete Verlangen der betroffenen Person erfüllt wird. Insbesondere die korrekte Identifizierung spielt eine große Rolle.

☐ **WER** soll die zu übertragenden Daten aushändigen? Falls mehrere Fachabteilungen (und der Datenschutzbeauftragte) von dieser Pflicht betroffen sind, so ist das kein simples Unterfangen. Wurde ein Leitfaden erarbeitet, der – im Sinne des Kapitel 12.7.1 – die konkrete Vorgehensweise festlegt?

☐ Die Daten welcher Verarbeitungen sind betroffen? Kann/will die betroffene Person die gewünschten Daten benennen? Zunächst muss geklärt werden, ob die bereits bestehenden Verarbeitungen (bzw. später neu hinzukommenden Verarbeitungen) überhaupt von dieser Export-Pflicht betroffen sind.

☐ Ja, es handelt sich um eine **automatisierte Verarbeitung.**

☐ Ja, die betroffene Verarbeitung basiert auf einer **(ausdrücklicher) Einwilligung** gemäß Artikel 6 (1a) / Artikel 9 (2a) oder auf einem **Vertragsverhältnis** gemäß Artikel 6 (1b).

☐ Ja, die betroffene Person hat die **sie selbst betreffenden** Daten **selbst bereitgestellt.** Also selbst eingetippt oder hochgeladen.

☐ Wenn alle drei obigen Bedingungen zutreffen, dann müssen die Daten tatsächlich exportiert werden. ACHTUNG:

☐ keine Betriebs- und Geschäftsgeheimnisse offenlegen (siehe Kapitel 9.2.2)!
☐ die Rechte Dritter achten!

☐ Der Datenexport wurde vorgenommen, und die Daten bereitgestellt:

Datum: …….. per

☐ Post ☐ Telefon ~~☐ Fax~~
☐ E-Mail (verschlüsselt), ☐ Website (verschlüsselt)
☐ Sonstiges: ….

☐ Die betroffene Person ist zufrieden? ☐ ja / ☐ nein, weil ….

Die bereitgestellten Daten werden zu Nachweiszwecken (z.B. für drei Jahre) archiviert?

☐ ja
☐ nein

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.12 Widerspruch bearbeiten [GVO_021]

Formulare

Gemäß Artikel 21 kann eine betroffene Person einer Verarbeitung widersprechen, sofern die Rechtsgrundlage der Verarbeitung auf **(a)** öffentlichen Interessen oder **(b)** berechtigten Unternehmensinteressen beruht. Die Person muss „eine besondere Situation“ nachweisen. Das Unternehmen kann dies ablehnen, wenn die Verarbeitung zwingend notwendig ist.

➔ Siehe Pflicht **[GVO_021]** auf Seite 93.

\PrivazyPlan\GVO_021
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Widerspruch einer betroffenen Person

Name der betroffenen Person (Nachname, Vorname): ……

☐ Das **Formular „Persönlichkeitsrechte erfüllen“** im Kapitel 12.1.5 des PrivazyPlan® wurde berücksichtigt. Dort finden sich viele wichtige Prüfungen, bevor/nachdem das konkrete Verlangen der betroffenen Person erfüllt wird. Insbesondere die korrekte Identifizierung spielt eine große Rolle.

Der Widerruf wurde gefordert am ……
per ☐ Post
☐ E-Mail
☐ Website
☐ Sonstiges: …

☐ Ja, es handelt sich wirklich um einen **Widerspruch** und nicht etwa um den **Widerruf einer Einwilligung**. Manchmal sind diese beiden Verlangen schwer zu unterscheiden (z.B., weil sich die betroffene Person unklar ausdrückt). Aber hier wird wirklich im Sinne der unten aufgeführten Punkte ein Widerspruch ausgesprochen! (Andernfalls käme die Pflicht **[GVO_007b]** zum Tragen, siehe Kapitel 4.5 Seite 148).

☐ Ja, es wurde nicht nur der Widerruf ausgesprochen, sondern auch eine (sofortige?) **Löschung** verlangt. Hier kommt die Pflicht **[GVO_017a]** zum Tragen (siehe Kapitel 2.8 Seite 75).

Dieses Verlangen wird zunächst dokumentiert ☐ auf Papier ☐ in einem Ticket-System [ID= ……]

Betroffen sind die folgenden Verarbeitungen: … [Es ist sehr wichtig hier präzise zu arbeiten. Leider sind die Formulierungen der betroffenen Personen oft zu allgemein. Finden Sie also genau heraus, gegen welche Verarbeitung widersprochen wird.]

Welche der zulässigen Widerspruchsmöglichkeiten wird wahrgenommen:

☐ gegen Verarbeitung im öffentlichen Interesse im Sinne des Artikel 6 (1e)

☐ gegen berechtigte Geschäftsinteressen im Sinne des Artikel 6 (1f)

☐ gegen Direktwerbung (Newsletter, Telefon, Post, etc., siehe Kapitel 9.6.2) im Sinne des Artikel 21 (2)

☐ gegen wissenschaftliche und historische Forschungszwecke im Sinne des Artikel 21 (6)

☐ Ja, die betroffenen Daten werden gemäß Artikel 18 (1d) „eingeschränkt“, solange das Verlangen der betroffenen Person geprüft wird. Hier kommt die Pflicht **[GVO_018]** ins Spiel (siehe Kapitel 2.10 Seite 80).

Es wurden Tatsachen dargelegt, die die „besondere Situation“ belegen:
[Es ist sehr wichtig hier präzise zu arbeiten. Es reicht in aller Regel nicht aus, dass eine betroffene Person pauschal widerspricht Das berechtigte Gegen-Interesse muss klar formuliert werden (dies können rechtliche, wirtschaftliche, ethische, soziale, gesellschaftliche oder familiäre Umstände sein). Nur dann können die Interessen abgewogen werden. Siehe hier.]
☐ nein / ☐ ja: …

Es gibt zwingende Gründe für das Unternehmen, die Verarbeitung fortzuführen:

☐ ja, und zwar: ☐ steuerliche Aufbewahrungsfrist ☐ Sonstiges: ….

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.13 Gemeinsame Verantwortlichkeit [GVO_026]

Formulare

Bisher wurde in diesem Kapitel nur die vertragliche Vereinbarung thematisiert. Dieses Thema wird aber immer wichtiger (siehe Google Analytics), daher gibt es nun verschiedene Unterkapitel.

Die gemeinsame Verantwortlichkeit gemäß Artikel 26 soll es mehreren Unternehmen erlauben, eine Verarbeitung gemeinsam – und zu den jeweils eigenen Zwecken – durchzuführen. In Hinblick auf Schadenersatzforderungen haften alle Verantwortlichen gemäß Artikel 82 (4) 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.

➔ Siehe Pflicht **[GVO_026]** auf Seite 192.

➔ Ein Überblick über alle Arten des Daten-Transfers findet sich auf Seite 530.

12.13.1 Prüfkatalog zur gemeinsamen Verantwortlichkeit

Das Datenschutzrecht kennt zahlreiche Möglichkeiten, um die Weitergabe von personenbezogenen Daten an einen anderen „Verantwortlichen“ rechtskonform zu gestalten. Seit dem Jahr 2019 rückt die „gemeinsame Verantwortlichkeit“ gemäß Artikel 26 immer weiter in den Vordergrund. Der (vorläufige) Höhepunkt ist erreicht, als die Hamburger Aufsichtsbehörde im November 2019 quasi „offiziell“ eine gemeinsame Verantwortlichkeit im Zusammenhang mit Google Analytics feststellt.

Weil eine gemeinsame Verantwortlichkeit aufwändige vertragliche Regelungen nach sich ziehen (und gemäß Artikel 82 (4) eine gemeinsame Haftung hinsichtlich Schadenersatzforderungen bedeutet, siehe Seite 588), wird man sorgfältig überlegen, ob man mit anderen Unternehmen gemeinsam verantwortlich sein möchte (siehe Datenschutz-Berater 07-08/2020 Seite 168-170).

Leider lässt sich im März 2020 nicht sicher vorhersagen, wie die Aufsichtsbehörden oder Gerichte (so z.B. der EuGH) zu ihren jeweiligen Einschätzungen gelangen. [114] Insofern ist es alles andere trivial einen solchen Kriterienkatalog zu erstellen. Trotzdem wollen wir im Folgenden einen Versuch vagen.

\PrivazyPlan\GVO_026
… dort können Sie die ausgefüllten Checklisten speichern.
Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Prüfkatalog zur gemeinsamen Verantwortlichkeit

Die folgende Checkliste soll objektiv klären, ob der Datentransfer an einen Dritten ggf. eine „gemeinsame Verantwortlichkeit“ darstellt.

Es geht um diese Verarbeitung: …… (nennen Sie hier den Namen)

a) Keine gemeinsame Verantwortlichkeit liegt vor, wenn…

☐ Es existiert ein Vertrag zur **Auftragsverarbeitung** im Sinne der Pflicht **[GVO_028]** auf Seite 207. Insofern kann eine gemeinsame Verantwortlichkeit ausgeschlossen werden. Die Verantwortung für die Daten wird zu 100% vom Auftraggeber getragen.
(ACHTUNG: Google Analytics ist nach Ansicht der Datenschutzkonferenz eine gemeinsame Verantwortlichkeit, siehe hier!

☐ Die Datenweitergabe an den Dritten ist eine „**Offenlegung durch Übermittlung**“ gemäß Artikel 4 Nr. 2. Im gewissen Sinne handelt es sich hier um eine „Einbahnstraße“. Dies bedeutet: Wenn die Daten einmal transferiert sind, dann haben Sie damit keinerlei Berührung mehr (auch nicht in Form von Statistiken). Hier gilt das Prinzip „*aus den Augen, aus dem Sinn*“. Demnach wäre dies eine „Übermittlung“ wie dies im Merkblatt für Datentransfers auf Seite 531 ausführlich beschrieben wird (und wo viele Beispiele genannt werden). Der Daten-Empfänger trägt 100% der Verantwortung.

[Ab hier eine Lücke aufgrund der Leseprobe...]

[114] Die Begründungen in den diversen EuGH-Urteilen sind äußerst dünn und thematisieren in keiner Weise, dass man Daten auch an einen Dritten „übermitteln“ kann. Auch die HH-Aufsichtsbehörde würdigt dieser Einschätzung keinen einzigen Satz.

12.14 Auftragsverarbeitung… [GVO_028], [GVO_028a]

Formulare

Gemäß Artikel 28 kann der Verantwortliche externe Dienstleister einbinden, um personenbezogene Daten dort verarbeiten zu lassen. Geschieht dies streng weisungsgebunden, so spricht man von einer Auftragsverarbeitung („Outsourcing“). Für diese Offenlegung von Daten bedarf es keiner Einwilligung durch die betroffenen Personen; der Auftragsverarbeiter (siehe Artikel 4 Nr. 8) ist gemäß Artikel 4 Nr. 10 kein Dritter! Allerdings entsteht ein großer bürokratischer Aufwand, bevor eine Auftragsverarbeitung rechtskonform durchgeführt werden kann.

➔ Siehe Pflicht **[GVO_028]** auf Seite 207.
Konkrete **Vertragsvorlagen** werden genannt auf Seite 211.

Im Internet finden sich zahlreiche Vertragsvorlagen (siehe Seite 211). Wir empfehlen derzeit die Vorlage der GDD:

\PrivazyPlan\GVO_028
Dort finden Sie die GDD-Vertragsvorlage im MS-Word-Format. Wir haben das Dokument insofern optimiert, als dass alle individuellen Bestimmungen in einer Anlage gesammelt werden. Das erhöht den Komfort und die Übersichtlichkeit.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Gemäß Artikel 28 kann der Verantwortliche externe Dienstleister einbinden, um personenbezogene Daten dort verarbeiten zu lassen. Geschieht dies streng weisungsgebunden, so spricht man von einer **Auftragsverarbeitung** („Outsourcing“). Für diese Offenlegung von Daten bedarf es keine Einwilligung durch die betroffenen Personen. Allerdings entsteht ein großer bürokratischer Aufwand, bevor eine Auftragsverarbeitung rechtskonform durchgeführt werden kann.

12.14.1 Einleitung

Die in dem hier vorliegenden Dokument beschriebene Art des Outsourcings wird bis zum 25.05.2018 gemäß § 11 BDSG-alt als „**Auftragsdatenverarbeitung**“ behandelt.

Ab dem 25.05.2018 gilt dann die europäische Datenschutz-Grundverordnung, die dieses Outsourcing gemäß Artikel 28 als „**Auftragsverarbeitung**“ bezeichnet.

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.15 Verarbeitungen… [GVO_030], [GVO_030a]

Formulare

Für die **Verantwortlichen** einer Verarbeitung gilt:
Die Dokumentation der Verarbeitungstätigkeiten gemäß Artikel 30 durch den Verantwortlichen ist besonders wichtig. Jede einzelne Verarbeitung muss präzise dokumentiert werden. Ohne eine solche Dokumentation kann das Unternehmen nicht garantieren, dass der Umgang mit personenbezogenen Daten datenschutzrechtlich zulässig ist.
➔ Siehe Pflicht **[GVO_030]** auf Seite 110.

Für die **Auftragsverarbeiter** gilt:
Im Rahmen von Outsourcing hat jeder Auftragsverarbeiter gemäß Artikel 30 (2) seine Dienstleistungen zu dokumentieren. Dies umfasst auch die Namen und Kontaktdaten seiner Auftraggeber. Somit hat der Auftragsverarbeiter stets eine genaue Übersicht darüber, welche Leistungen er für welche Kunden erbringt.
➔ Siehe Pflicht **[GVO_030a]** auf Seite 116.

Anmerkung: Das Verarbeitungsverzeichnis des Auftragsverarbeiters gemäß der Pflicht **[GVO_030a]** bedarf keines expliziten Formulars. Die geforderte Dokumentation kann in MS-Excel erledigt werden (siehe Seite 116)

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.16 Informations-Sicherheit… [GVO_032]

Formulare

Es sind technische und organisatorische Maßnahmen zu treffen, um eine sichere Datenverarbeitung gemäß Artikel 32 (1) dauerhaft sicherzustellen. Eine diesbezügliche Nachweis-, Überwachungs- und Aktualisierungspflicht fordert der Artikel 24 (1). Dabei muss das Risiko der jeweiligen Datenverarbeitung angemessen berücksichtigt werden. Nur ein „Informations-Sicherheits-Managementsystem“ (ISMS) kann all dies gewährleisten.

➔ Siehe Pflicht [GVO_032] auf Seite 158.

Hier werden verschiedene Formulare rund um das Thema „Informations-Sicherheit“ zur Verfügung gestellt:

12.16.1 Informations-Sicherheits-Managementsystem auswählen

Informations-Sicherheit…

➔ Siehe Pflicht [GVO_032] auf Seite 158.

➔ Siehe die Fachinformationen zu den Optionen eines ISMS im Kapitel 13.4 auf Seite 524.

\PrivazyPlan\GVO_032
… dort finden Sie die folgende Checkliste als MS-Word Dokument.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Auswahl eines Informations-Sicherheits-Managementsystems (ISMS)

Es sind technische und organisatorische Maßnahmen zu treffen, um eine sichere Datenverarbeitung gemäß Artikel 32 (1) dauerhaft sicherzustellen. Eine diesbezügliche Nachweis-, Überwachungs- und Aktualisierungspflicht fordert der Artikel 24 (1). Dabei muss das Risiko der jeweiligen Datenverarbeitung angemessen berücksichtigt werden. Nur ein „Informations-Sicherheits-Managementsystem“ (ISMS) kann all dies gewährleisten.

a) Grobe Planung

Die Auswahl eines Informations-Sicherheits-Managementsystems wird im Kapitel 13.4 ausführlich thematisiert.

☐ Dieses Dokument haben wir gelesen, und wir berücksichtigen es bei unseren Planungen. (In der kostengünstigen PrivazyPlan®-Epressversion steht dieses Kapitel nicht zur Verfügung.)

Wir sind zum folgenden Ergebnis gekommen:

☐ Wir werden **keinerlei ISMS** aufsetzen. Begründung: …

☐ Wir nutzen eine **kurze Checkliste**, weil unser Unternehmen minimale Anforderungen an die Informationssicherheit hat Wir speichern nur wenige Daten und diese Daten sind nicht „sensibel“. ☐ Diese Einschätzung haben wir uns von einem externen Fachmann bestätigen lassen.

☐ Konkret nutzen wir die **Ultrakurz-Checkliste** gemäß Kapitel 12.16.2.

☐ Konkret das Standard-Dokument
„interview_tom_domaene.doc“ von DSB-MIT-SYSTEM®
mit beispielhaften technisch-organisatorischen Maßnahmen
auf ca. 24 Seiten.

☐ Konkret diese Checkliste: …….

☐ Wir nutzen die **ISA+ - Informations-Sicherheits-Analyse** gemäß Kapitel 13.4.2 Ein beispielhaftes Dokument befindet sich im Unterverzeichnis

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.17 Datenschutzverletzung, Beschwerde [GVO_033]

Formulare

Das hier vorliegende Statusblatt soll einen groben Überblick darüber liefern, wie man mit einer Datenschutzverletzung bzw. einer Beschwerde umgehen kann.

12.17.1 Dokumentation einer Datenschutzverletzung

Datenschutzverletzung, Beschwerde

Dieses Formular deckt drei Pflichten ab:

- Gemäß Artikel 33 (1) muss eine Datenschutzverletzung innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden, sofern voraussichtlich ein mittleres oder großes Risiko für die „Rechte und Freiheiten" der betroffenen Personen besteht. Das Unternehmen muss also zunächst eine Risikoprognose erstellen und dann ggf. eine Meldung machen.
  ➔ Siehe Pflicht **[GVO_033]** auf Seite 170.

- Gemäß Artikel 33 (5) muss der Verantwortliche alle Datenschutzverletzungen sehr detailliert dokumentieren. Das gilt für alle Datenschutzverletzungen gemäß Artikel 4 Nr. 12 (egal, ob geringes, mittleres oder hohes Risiko). Die Aufsichtsbehörde darf diese Dokumentation gemäß Artikel 58 (1a) jederzeit einsehen.
  ➔ Siehe Pflicht **[GVO_033a]** auf Seite 174.

- Bei einer Datenschutzverletzung mit voraussichtlich hohem Risiko muss gemäß Artikel 34 (1) die betroffene Person unverzüglich benachrichtigt werden. Eine öffentliche Bekanntmachung kann notwendig sein, wenn die einzelnen Personen nicht erreicht werden können.
  ➔ Siehe Pflicht **[GVO_034]** auf Seite 178.

Auf Seite 429 wird aufgezeigt, wie man Datenverluste vermeiden bzw. erkennen kann.

\PrivazyPlan\GVO_033
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Dokumentation einer Datenschutzverletzung gemäß Artikel 33 (5)

Gemäß Artikel 33 (5) muss jede Datenschutzverletzung dauerhaft dokumentiert werden. Dies geschieht mit dem hier vorliegenden Formular. Das ausgefüllte Dokument wird an vertraulicher und sicherer Stelle für 3 Jahre aufbewahrt (auf Basis von § 195 BGB bzw. § 31 OwiG).

[Tipp: Es ist sinnvoll, dass Sie die nicht-zutreffenden Texte nicht löschen, sondern durchstreichen. Dadurch wird transparent, was alles NICHT zutrifft.]

a) Grundlegende Informationen

Im Folgenden werden die ganz grundlegenden Informationen gesammelt. Inhaltlich orientiert sich dies am Artikel 33 (3) und könnte somit ggf. zur Meldung an die Aufsichtsbehörde genutzt werden.

☐ Wurde ein Datenschutz-Konzept erarbeitet (siehe Kapitel 12.17.3 auf Seite 447 im PrivazyPlan®)? Wenn ja, dann sollte dies nun angewendet werden.

☐ Name des verantwortlichen Unternehmens: …

Wo ist es passiert:
☐ Personalabteilung
☐ Marketing / Vertrieb
☐ Kundenbetreuung
☐ IT-Abteilung
☐ Betriebsrat [Falls dieses Formular vom Betriebsrat ausgefüllt wird: Möglicherweise wurde im Rahmen der *„Vereinbarung zur gemeinsamen Zuständigkeit von Arbeitgeber/-in und Betriebsrat gemäß § 79a BetrVG"* (siehe Kapitel 12.21.1) vereinbart, dass der Arbeitgeber über Datenschutzverletzungen informiert werden soll.]
☐ Sonstige Abteilung/Stelle: ....
☐ Neu im Mai: Bei einem Auftragsverarbeiter: ...

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.18 Risiko, Folgenabschätzung, Konsultation… [GVO_035], [GVO_036]

Formulare

Hier werden verschiedene Formulare rund um das Thema „Risiko“ zur Verfügung gestellt:

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.19 Benennung eines Datenschutzbeauftragten [GVO_037]

Formulare

Die eventuelle Verpflichtung zur Benennung eines Datenschutzbeauftragten muss sorgsam geprüft werden.
Die zu benennende Person muss die hohen Anforderungen an Zuverlässigkeit und Fachkunde erfüllen.

➔ Siehe Pflicht **[GVO_037]** auf Seite 235.

Bitte beachten Sie unbedingt das sehr aussagekräftige „WP 243“ der Artikel-29-Datenschutzgruppe (siehe Seite 599). Dort wird auf Seite 6 u.a. gefordert, dass **auch die fehlende Notwendigkeit** der Benennung eines Datenschutzbeauftragten schriftlich dokumentiert und regelmäßig überprüft werden soll.

\PrivazyPlan\GVO_037
… dort können Sie die ausgefüllte Checkliste speichern.
Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Benennung eines Datenschutzbeauftragten („DSB“)

Unternehmen: ……(genaue Firmierung)

a) Notwendigkeit eines DSB

Aus welchen Gründen muss/soll ein DSB benannt werden? Die unzutreffenden Punkte werden durchgestrichen.

☐ Die Kerntätigkeit des Unternehmens umfasst gemäß Artikel 37 (1b) eine regelmäßige und systematische Überwachung von Personen. [137] [138]

☐ Die Kerntätigkeit des Unternehmens umfasst gemäß Artikel 37 (1c) die umfangreiche Verarbeitung von „sensiblen“ Daten. [139]

☐ In Deutschland gibt es die AUSNAHME für einen einzelnen Arzt oder Rechtsanwalt.

☐ In Deutschland sind ab dem 26.11.2019 gemäß § 38 Abs. 1 BDSG mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

☐ In Deutschland finden Verarbeitungen statt, die gemäß Artikel 35 einer Datenschutz-Folgenabschätzung unterliegen (siehe Kapitel 6.1 Seite 182) und demnach gemäß § 38 Abs. 1 BDSG die Benennung eines DSB erfordern.
Bei einzelnen Ärzten und Rechtsanwälten ist gemäß Erwägungsgrund 91 keine Datenschutz-Folgenabschätzung notwendig (siehe Seite 183).

☐ In Deutschland finden ab dem 25.05.2018 Verarbeitungen statt zum Zweck der geschäftsmäßigen Übermittlung bzw. der Markt- oder Meinungsforschung, sodass gemäß § 38 Abs. 1 BDSG die Benennung eines DSB erforderlich ist.

b) Für die Stelle des DSB gilt:

☐ es wird **KEIN** DSB benannt, weil es keine gesetzliche Pflicht gibt
☐ Der Geschäftsleitung ist bewusst, dass trotzdem alle 50 Pflichten gelten.

☐ es wird gemäß Artikel 37 (4) auf **freiwilliger** Basis ein DSB benannt

[Ab hier eine Lücke aufgrund der Leseprobe...]

[137] Nicht zu den „Kerntätigkeiten“ gehört beispielsweise die Entlohnung der Mitarbeiter. Insofern sind manche frühen Einschätzungen in der deutschen Fachliteratur unzutreffend (siehe „WP 243“ Seite 8).
[138] Eine solche Überwachung ist beispielsweise verfolgende E-Mail-Werbung (wer öffnet welchen Newsletter?), datengesteuerte Marketingaktivitäten, Scoring zu Zwecken der Risikobewertung (Kreditvergabe, Versicherungsprämien, Betrugsverhinderung, Geldwäsche-Prävention), Standortverfolgung, Treueprogramme, verhaltensbasierte Werbung, Wearables, Überwachungskameras. Siehe „WP 243“ Seite 10.
[139] Das „WP 243“ nennt auf Seite 9 beispielsweise Krankenhäuser, den öffentlichen Personen-Nahverkehr (ÖPNV) oder das Versicherungs- oder Bankenwesen oder Telefon- bzw. Internetdienstleister.

12.20 Datentransfer (in ein Drittland) [GVO_044]

Formulare

Gemäß der Artikel 44, 45, 46, 47, 48 und 49 ist ein Transfer von personenbezogen Daten an Drittländer bzw. internationale Organisationen streng reglementiert. Dies ist wichtig, weil die Daten den EU-Rechtsraum verlassen und danach nicht mehr „kontrolliert" werden können.

Das EuGH-Urteil C-311/18 im Juli 2020 zum EU-US-PrivacyShield und den „alten" EU-Standardvertragsklauseln bringt den weltweiten Datentransfer ins Wanken (siehe Seite 496).

➔ Siehe Pflicht **[GVO_044]** auf Seite 222.

\PrivazyPlan\GVO_044
… dort können Sie die ausgefüllte Checkliste speichern.
Sie finden dort auch alle Checklisten im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

12.20.1 Checkliste zur Zulässigkeit eines Drittland-Datentransfers

Datentransfer (in ein Drittland)

Es gibt eine **Voraussetzung für die systematische Anwendung** der hier vorliegenden Checkliste: Identifizieren Sie alle Datentransfers in Drittländer (USA, Schweiz etc.)! Berücksichtigen Sie dabei unbedingt auch jene Datentransfers, die ggf. durch Ihre Auftragsverarbeiter stattfinden! Beispielsweise hat sich im Frühjahr 2020 herausgestellt, dass (fast alle) europäische Videokonferenz-Anbieter immer auch US-amerikanische Clouddienste (siehe Seite 662) nutzen.

Die Aufsichtsbehörden erwarten eine **dokumentierte Begründung**, warum ein Drittland-Datentransfer vom Verantwortlichen für rechtmäßig gehalten wird. Andernfalls kann z.B. eine US-Datenübermittlung als unzulässig eingeschätzt werden (siehe die Reaktion auf eine Beschwerde hinsichtlich MailChimp bei der bayerischen Aufsichtsbehörde am 15.03.2021). [142] Insofern ist die folgende Checkliste sehr hilfreich.

Prüfung eines Drittland-Datentransfers gemäß Artikel 44

Unternehmen: ……(genaue Firmierung)

Name der Verarbeitung: ……

Der Drittland-Datentransfer wird durchgeführt:
☐ durch uns selbst
☐ durch einen Externen (Auftragsverarbeiter, anderen (Mit-) Verantwortlichen) [143]

Der Drittland-Datentransfer hat die folgende Ausprägung (siehe Seite 530):
☐ **gemeinsame Verantwortlichkeit** mit einem Dritten (siehe Seite 192)
☐ **Auftragsverarbeitung** durch einen Dienstleister (siehe Seite 207)
☐ **Übermittlung** an einen eigenverantwortlichen Dritten (siehe Seite 533)
☐ **Berechtigte Interessen in der Unternehmensgruppe** (siehe Seite 553)

Empfangende Drittländer: ……

[142] Die Aufsichtsbehörde sah hier nur ein „leichtes Maß an Fahrlässigkeit" hinsichtlich Daten, deren „Sensibilität noch verhältnismäßig überschaubar ist"; daher wurde kein Bußgeld verhängt. Leider ist völlig unklar, ob es eine explizite Drittland-Einwilligung gemäß Artikel 49 (1a) gab, und ob dies einen Einfluss auf die Einschätzung der Aufsichtsbehörde gehabt hätte. Diese fehlenden Details lassen sich wohl dadurch erklären, dass hier das Antwortschreiben an die betroffene Person vorliegt... diese ist stets oberflächlicher formuliert als die Anschreiben an den Verantwortlichen.

[143] Dies ist ein wichtiger Punkt. Der Drittland-Datentransfer kann auch durch ein anderes Unternehmen erfolgen, wobei dies eine logische Konsequenz unserer eigenen Datenverarbeitung darstellt. Daher kann man jenen Drittland-Datentransfer nicht einfach ignorieren. Dies wird beispielsweise im Artikel 28 (3a) und im Artikel 28 (4) thematisiert. Wie/Warum es auch immer zu einem Drittland-Datentransfer kommen kann, so muss die betroffene Person gemäß Artikel 13 (1f) darüber vorab eine Auskunft erhalten.

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.21 Formulare zu den „weichen“ Pflichten [AUX_001] etc.

Formulare

Neben den ca. 50 bußgeldbewehrten Pflichten gibt es im Datenschutz auch einige wichtige „Strategien“, um das Gesamtziel erreichen zu können. Diese Strategien werden hier im PrivazyPlan® als „weiche“ Pflichten bezeichnet und erhalten das Kürzel „[AUX_001]“ etc.

Im Kapitel 12.1.7 ab Seite 319 wird all dies detailliert beschrieben.

Auch für diese „weichen“ Pflichten können Formulare und Checklisten erforderlich sein. Dafür ist dieses hier vorliegende Kapitel 12.21 zuständig.

12.21.1 Gemeinsame Zuständigkeit mit dem Betriebsrat [AUX_004]

Formulare zu den „weichen“ Pflichten

Der Betriebsrat ist ein datenschutzrechtlicher Teil des Arbeitgebers; so hat es die Novellierung des BetrVG durch das Betriebsrätemodernisierungsgesetz am 17.06.2021 festgelegt.

Die Gesetzesbegründung besagt unter anderem: „*Daher sind Arbeitgeber und Betriebsrat bei der Erfüllung der datenschutzrechtlichen Pflichten in vielfacher Weise auf gegenseitige Unterstützung angewiesen.*“ (siehe Seite 17). Genau darum geht es in der unten aufgeführten Vereinbarung.

(In gewisser Hinsicht gibt es hier eine Parallele zur „gemeinsamen Verantwortlichkeit“ gemäß Artikel 26 und der Pflicht [GVO_016] auf Seite 192. Auch dort bedarf es eines Vertrags zur Klärung der konkreten Details einer Zusammenarbeit. So gesehen handelt es sich hier gewissermaßen um eine Light-Version der gemeinsamen Verantwortlichkeit.)

Die folgende Vereinbarung ist ein unverbindlicher Vorschlag, um die gemeinsame Zuständigkeit von Arbeitgeber/-in und Betriebsrat zu regeln. Sie ist somit auch ein erster Anstoß, damit sich die beiden Parteien an einen Tisch setzen und über den (gemeinsamen) Datenschutz sprechen.

Die RDV 04/2021 liefert auf Seite 183f die Vorlage einer Betriebsvereinbarung, die mit der unten folgenden Vereinbarung vergleichbar ist.

\PrivazyPlan\AUX_004
… dort können Sie Ihre konkreten Arbeitsergebnisse speichern.
Sie finden dort auch alle Checklisten im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

Vereinbarung zur gemeinsamen Zuständigkeit von Arbeitgeber/-in und Betriebsrat gemäß § 79a BetrVG

Der/die Arbeitgeber/-in und der Betriebsrat einigen sich hiermit auf eine gemeinsame Zuständigkeit für den Betriebsrats-Datenschutz.

Sämtliche hier genannten Pflichten werden im Datenschutz-Praxisleitfaden PrivazyPlan® ausführlich erläutert und im Kapitel 12 mit Checklisten und Vorlagen ergänzt.

Datenschutz beim Betriebsrat regeln (Kapitel 12.1.7.4 im PrivazyPlan®)

Der § 79a BetrVG („Datenschutz“) besagt:

> *„Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten.*
> *Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung **Verantwortliche** im Sinne der datenschutzrechtlichen Vorschriften.*
> *Arbeitgeber und Betriebsrat **unterstützen** sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften.*
> *Die oder der **Datenschutzbeauftragte** ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen.*

[Ab hier eine Lücke aufgrund der Leseprobe...]

12.22 Datenschutz bei Telemedien und -Kommunikation [TTDSG]

Formulare

In Deutschland gilt seit dem 01.12.2021 ein neues Gesetz hinsichtlich des Datenschutzes und der Privatsphäre in der Telekommunikation und bei Telemedien: Das TTDSG (siehe Seite 269).

12.22.1 Dokumentation von Cookies (inkl. Einwilligung)

Formulare zum TTDSG

Das Thema „Cookies“ wird ausführlich ab Seite 633 beschrieben. Seit dem 01.12.2021 fallen Cookies unter dem § 25 TTDSG („Schutz der Privatsphäre bei Endeinrichtungen“).

\PrivazyPlan\zzz TTDSG_025
… dort können Sie die ausgefüllte Checkliste speichern. Sie finden dort auch diese Checkliste im MS-Word-Format.
(Diese Verzeichnisstruktur wird ab Seite 29 erklärt.)

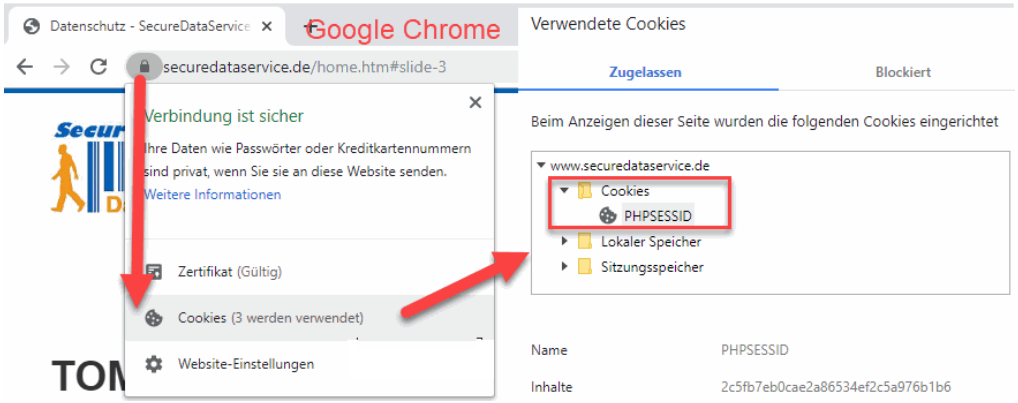
Dokumentation von Cookies (inkl. Einwilligung)

Gemeinsam mit Ihrem Webmaster können Sie die hier vorliegende Checkliste bearbeiten.

Es geht um diese Website: ……..

a) Identifizieren Sie alle Cookies

Nutzen Sie beispielsweise den Chrome-Browser, um die Cookies Ihrer Website zu identifizieren. Achten Sie unbedingt darauf, dass es keinerlei Content-Filter gibt, der dieses Ergebnis beeinträchtigt (wie z.B. das Ghostery-Addon im Firefox).



In der obigen Abbildung sehen sie, wo die Cookies zu finden sind. Die Punkte „Lokaler Speicher“ und „Sitzungsspeicher“ sind erstmal nicht Bestandteil dieser Checkliste (obwohl sich auch dort spannende Daten finden).

b) Einschätzen der Rechtsgrundlage

Jede Verarbeitung bedarf eine Rechtsgrundlage, wie es die Pflicht [GVO_006] fordert (siehe Seite 122). Bei den Cookies kommen dafür verschiedene Rechtsgrundlagen in Frage. Das ist ein wichtiger Punkt, denn das oben genannte EuGH-Urteil bezieht sich (ohne das so explizit zu erwähnen) nur auf die Einwilligungs-relevanten Cookies.

☐ § 25 Abs. 1 TTDSG: Welche Cookies sind **„nur“ nützlich bzw. hilfreich** (weil sie nicht den Ausnahmen des § 25 Abs. 2 TTDSG unterliegen) und müssen mit einer **Einwilligung** versehen werden?

……

☐ § 25 Abs. 2 Nr. 1 TTDSG: Welche Cookies sind für **die Datenübertragungs-Technik unbedingt erforderlich** (wie z.B. die IP-Adresse eines Streaming-Servers) und müssen NICHT mit einer Einwilligung versehen werden?

……

☐ § 25 Abs. 2 Nr. 2 TTDSG: Welche Cookies sind **für die Zurverfügungstellung unbedingt erforderlich** (wie z.B. der Warenkorb eines Onlineshops) und müssen NICHT mit einer Einwilligung versehen werden?

……

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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.

13.1.1 Änderungen in der Zukunft

Welche Änderungen im Datenschutz sind zukünftig zu erwarten? Hier richtet sich der Blick vor allem auf den EuGH, denn dessen Urteile haben inzwischen einen direkten Einfluss auf das Tagesgeschäft der Verantwortlichen (siehe das Urteil zu Safe-Harbor oder zur facebook-Fanpage, siehe Seite 197).

- Allem Voran ist natürlich die **ePrivacy-Verordnung** zu nennen, die zwar eine erhebliche Auswirkung auf den Datenschutz im Internet haben wird, aber deren Beschluss in den Sternen steht (siehe Seite 262).

- Derzeit ist eine **e-Evidence-Verordnung** in Diskussion, die u.a. für Onlineshops und Telekommunikations-Anbieter relevant sein könnte. Dann müssten Daten zur Strafverfolgung herausgegeben werden. Datenschützer sehen das kritisch. Eine Ähnlichkeit zum US-CLOUD-Act ist gegeben (siehe Seite 231).

13.1.2 Änderungen in der Vergangenheit

In dem hier vorliegenden Kapitel werden wichtige Neuerungen kontinuierlich dokumentiert. [Diese Liste wird kontinuierlich gestrafft und gekürzt, damit der Umfang auf wenige Seiten begrenzt ist.]

- **Neue EU-Standarddatenschutzklauseln im Juni 2021**
  Am 04.06.2021 teilt die EU-Kommission hier mit, dass ein neue Vertragswerke zum Datentransfer in Drittländer (siehe ab Seite 533) beschlossen wurden.

  Ein erster, grober Blick macht aber schon klar: Diese Verträge können nicht die Tatsache aus der Welt schaffen, dass die USA (nach Aussage des EuGH) ein Überwachungsstaat sind. In der Juli-Ausgabe des PrivazyPlan® werden wir ausführlich berichten.

- **Gesetz zu Telekommunikation und -Medien (TTDSG) am 19.05.2021**
  Die deutsche Gesetzgebung zu Telekommunikation und Telemedien wurde grundlegend überarbeitet und an europäisches Recht angepasst. Siehe Seite 269.

  Am 19.05.2021 wurde das TTDSG beschlossen und ab dem 01.12.2021 wird es angewendet. Es regelt den Datenschutz in Telekommunikations- und Telemedien-Diensten. Hiervon sind insbesondere Websites und Apps betroffen (siehe die „weiche“ Pflicht **[AUX_005]** auf Seite 321).

  Für Betreiber von Websites und Apps ändert sich im Grunde genommen nicht viel. Es bleibt bei der Einwilligung als Rechtsgrundlage für Cookies, allerdings droht gemäß § 28 TTDSG bei Zuwiderhandlung ganz konkret ein Bußgeld von bis zu 300.000 €. Auch der fehlerhafte Umgang mit Daten zur Wahrung des Jugendschutzes ist nun bußgeldbewehrt.

  Weitere Details finden sich u.a. in der 9-seitigen GDD-Praxishilfe „TTDSG im Überblick“.

  Aus dem TTDSG ergeben sich in Deutschland zwei neue bußgeldbewehrte Pflichten (siehe Seite 271) und die Pflicht zur Benennung einer verantwortli-

[Ab hier eine Lücke aufgrund der Leseprobe...]

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.

13.2.1 Was ist Compliance? Warum ist das Thema wichtig?

Compliance

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 strafbewährt sind oder Geldbußen nach sich ziehen könnten, 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.[149]

Dies wird zusätzlich durch den Artikel 24 (1) verstärkt, der besagt:
„*Der Verantwortliche setzt […] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert*“.

Im Rahmen des PrivazyPlan® wird dies berücksichtigt in der Pflichten **[GVO_005]** ab Seite 102 und **[AUX_008]** ab Seite 323.

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 irgendwie bezeichnend, dass man in Deutschland kein entsprechendes Wort für „Compliance“ hat.

In vielerlei Hinsicht lässt die DS-GVO keinen Zweifel darüber, dass Geldbußen und Schadenersatzforderungen drohen (siehe ab Seite 575).

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) Geldbußen gemäß § 43 BDSG-alt verhängten. Vorbei sind die Zeiten, wo Schadenersatzforderungen gemäß § 7 BDSG-alt nur bei nachweisbaren materiellen Schäden möglich waren.

[149] 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.

[Ab hier eine Lücke aufgrund der Leseprobe...]

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 zugreifen?

➔ In der Einleitung auf Seite 12 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.

In der Ping 03/2019 Seite 115-123 werden insgesamt 14 Kommentare vorgestellt („Hypertrophie der Kommentarliteratur“). Insgesamt 275 Autoren haben fast 19.000 Seiten geschrieben, wofür der Leser insgesamt ca. 1.900 € investieren müsste.

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.

Datenschutz

- „**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“**, Auernhammer
  Ca. 2.700 Seiten, 7. Auflage, 154 € (~ Februar 2020)

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.4 Informations-Sicherheits-Managementsysteme (ISMS)

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 158.

➔ Ein beispielhaftes Formular zur Auswahl eines ISMS findet sich im Kapitel 12.16 auf Seite 424.

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

Wie geht man dieses Thema überhaupt an? Ein lesenswerter Artikel dazu findet sich hier.

13.4.1 Auflistung der technisch-organisatorische Maßnahmen

Nur der Vollständigkeit halber sei diese Auflistung der TOM 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 12.16.2 auf Seite 426 zur Verfügung.

- **Kurz-Checkliste der VdS**
  In dem Anforderungskatalog der VdS 10020 (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

Station 4: IT-Sicherheit dauerhaft sicherstellen

Die IT-Sicherheitsmaßnahmen müssen systematisch betrieben und dokumentiert werden. Die allermeisten Unternehmen haben sich darauf noch nicht eingestellt. Daher weisen wir hiermit nochmals explizit darauf hin.

Das Minimum ist der ISA⁺-Fragebogen (siehe hier).

< Zurück • Home • Weiter >

Die folgenden beiden Fragebögen sind zwar kein vollwertiges 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 Auftragsverarbeiter im Sinne Artikel 28 DS-GVO einzusetzen, sollte man mindestens einen solchen Nachweis fordern (siehe Pflicht **[GVO_028]** auf Seite 207).

- **ISA⁺ - Informations-Sicherheits-Analyse (zertifizierbar) !!!**
  Mit diesem Fragenkatalog werden die 50 wichtigsten Aspekte der IT-

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.5 Daten-Transfer – ein Merkblatt

Fachinformationen

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

Bis zur Februar-Ausgabe des PrivazyPlan® wurde von einer „Weitergabe“ gesprochen. Nun nutzen wir den Begriff des „Transfers“. Das hat verschiedene Gründe (unter anderem ist der Begriff internationaler und ist somit im multinationalen Konzern besser anwendbar).

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

Das folgende Kapitel 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.

In Deutschland droht der § 42 BDSG mit einer **Freiheitsstrafe** von bis zu 3 Jahren, wenn personenbezogene Daten in großer Anzahl und gewerbsmäßig zu Unrecht an Dritte übermittelt werden (oder Dritten zugänglich gemacht werden).
Zu dieser Situation kann es eventuell auch dann kommen, wenn beispielsweise eine Auftragsverarbeitung ohne den notwendigen Vertrag durchgeführt wird und somit de facto der Tatbestand einer „Übermittlung“ angenommen werden muss.

ACHTUNG Dauer-Baustelle: Der Austausch von personenbezogenen Daten zwischen verschiedenen Unternehmen ist mitunter ein schwieriges Thema. In vielen Szenarien kann man trefflich streiten, welches der unten folgenden Möglichkeiten zutreffend ist. Exemplarisch sei der „Geschäftsbesorgung-Vertrag“ genannt (siehe Seite 195).
Durch die DS-GVO hat sich die Situation verschärft, weil sie sprachlich unscharf ist und zusätzliche Konstrukte bietet (z.B. die „gemeinsame Verantwortlichkeit“). Die Aufsichtsbehörden halten sich dezent zurück.

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente: ● Ausführliche Überlegungen zu den vielen möglichen Datentransfers in Datenschutz-PRAXIS 12/2020 Seite 5-7 ● 48-seitiger EDPB-Guideline 2020-07 mit zahlreichen Aspekten zur Verantwortlichkeit (mit automatisierter Übersetzung durch www.deepL.com) in Verbindung mit hilfreicher 9-seitiger FAQ aus Baden-Württemberg im Oktober 2020 ● FAQ zur Abgrenzung der Auftragsverarbeitung der Bayerischen Aufsichtsbehörde im Juli 2018.

Wie könnte man die drei wichtigsten Daten-Transfers **ganz grob charakterisieren**? Hier wird ein Versuch unternommen, der aber lediglich als eine laienhafte Analogie zu verstehen ist (und keinen rechtsverbindlichen Charakter hat):

[Ab hier eine Lücke aufgrund der Leseprobe...]

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 182) und Kapitel 13.21 ab Seite 667). Leider ist die objektive Einschätzung eines Risikos eine schwierige Angelegenheit, weil mit vielen unbestimmten Begriffen gearbeitet werden muss.

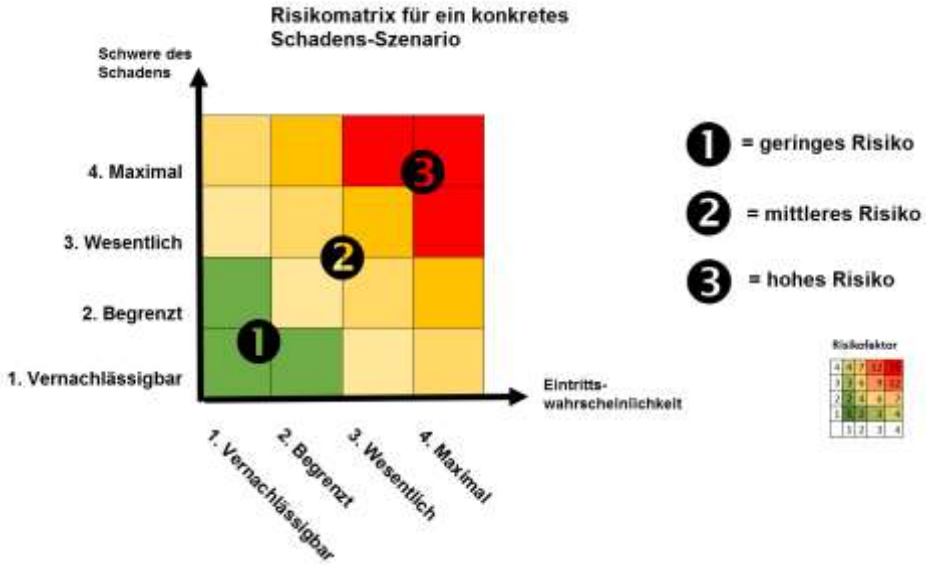
Die Risikoeinschätzung spielt unter anderem eine wichtige Rolle

- in der DS-GVO im Artikel 32, der letztlich für jede (Daten-) verarbeitung fordert, dass die technisch-organisatorischen Maßnahmen gemäß der Verordnung erfolgen. Siehe Pflicht **[GVO_032]** auf Seite 158. Eine dazugehörige Nachweis- und Optimierungspflicht ist im Artikel 24 gefordert.
- 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 174.
- 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 182.
- 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 524.

Viele Fachleute schlagen eine Risikomatrix (bzw. „Risiko-Landkarte“) 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

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.7 Aufbewahrungs- und Löschfristen (Beispiele)

Fachinformationen

Der Artikel 17 (1a) verlangt, dass personenbezogene Daten zu löschen sind, wenn der Zweck der Verarbeitung nicht mehr gegeben ist. Siehe Pflicht **[GVO_017]** auf Seite 72.

Die DS-GVO nennt keine konkreten Löschfristen. Daher muss man in anderen Gesetzen suchen.

Die Löschfristen sind für ein **Löschkonzept** wichtig (siehe Beispielformular auf Seite 363).

In Deutschland gelten die unten folgenden Beispiele. Es kann sein, dass zukünftig einige der hier genannten Fristen entfallen, weil die deutschen Gesetze novelliert werden (oder durch EU-Verordnungen ersetzt werden).

Die konkrete Nennung von Aufbewahrungsfristen ist nicht ganz einfach. Zum einen können sich die gesetzlichen Grundlagen ändern, zum anderen ist die Zuordnung zur jeweiligen Datenkategorie (und dazu zur jeweiligen Aufbewahrungsfrist) nicht immer ganz klar. [159]

Im Zweifelsfall sollte man annehmen, dass sich die Dauer der Aufbewahrung an der jeweils längsten Frist orientiert. (Die folgenden Fristen sind teilweise der Webseite www.reisswolf.de entnommen)

Internet und Telekommunikation (sofort)

- Kommunikations-Verbindungsdaten (sofern nicht für Abrechnung etc. benötig) § 96 TKG
- Webseiten-Nutzungsdaten (sofern nicht für Abrechnung etc. benötigt)

Internet (7 Tage)

- Logfiles des Webservers dürfen 7 Tage aufbewahrt werden (BGH-Urteil vom 13.01.2011, Az. III ZR 146/10) [160] Bestätigt durch eine ~~Pressemitteilung~~ aus Rheinland-Pfalz. Siehe auch hier.

Logfiles, Protokolldaten, Kontrolldaten (Tage bis Jahre)

Die Aufbewahrungsfristen von allgemein betriebsüblichen Logfiles, wie z.B. Firewalls, Zugriffsberechtigungen etc., sind pauschal kaum zu bestimmen. [161] Von zentraler Wichtigkeit ist der § 31 BDSG-alt, wo sich zahlreiche Erläuterungen finden (siehe Kapitel 7.12 im TOM-Guide®).

- 42 Tage können für allgemein betriebliche Logfiles realistisch sein [162]

Diverses (3 Monate)

- Informationen zum Tätigkeitsausschluss einschlägig vorbestrafter Personen gemäß § 72a SGB VIII aus Sicht des Paritätischen Gesamtverbandes in seiner Arbeitshilfe auf Seite 6. Die Frist zählt ab dem Ende des Beschäftigungsverhältnisses.

Bewerbungen (4 Monate)

- Die Bewerbungsunterlagen von abgelehnten Bewerbern sollten nach 4 Monaten vernichtet werden (angelehnt an die Klagefrist gemäß AGG). Mit Einwilligung ist natürlich eine längere Aufbewahrung möglich. Siehe ZD 05/2015 Seite 6f.

Internet (6 Monate)

- Abrechnungsdaten für genutzte Telemedien (§ 15 Abs. 7 TMG). Der Rest des TMG ist aber nicht anwendbar, siehe Seite 267.
- Bewerbungsunterlagen (§ 15 AGG mit kleinem „Sicherheitszuschlag“) [163]

---

[159] Ausführliche Liste der Aufbewahrungsfristen im Gesundheitsbereich unter www.kvhb.de/aufbewahrungsfristen und hier.

[160] Auch normale Webseiten-Betreiber dürfen 7 Tage speichern. Siehe www.youngdata.de/datenschutzerklaerung

[161] Die Orientierungshilfe „Protokollierung“ des Düsseldorfer Kreises aus dem Jahr 2009 (PDF) liefert grobe Kriterien für Löschfristen, aber keine konkreten Beispiele.

[162] Siehe Datenschutz-PRAXIS 09/2013 Seite 11; die 42 Tage ergeben sich aus einem 4-wöchigen Intervall der Logfile-Prüfungen und einem 2-wöchigen Zeitraum für die sachliche Überprüfung. Ebenso in DuD 12/2011 Seite 893. Auch in DIN-„Leitlinie zur Entwicklung eines Löschkonzepts“

[163] Siehe „Löschung von Bewerberdaten“ in Bayerischem Tätigkeitsbericht 2011-2012 Kapitel 13.1 (sollte eine längere Aufbewahrung gewünscht sein, so teilt man dies mit und bietet ein Widerspruchsrecht an)

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.8 Berechtigte Interessen einer Unternehmensgruppe

Fachinformationen

Die Datenübermittlung innerhalb der Unternehmensgruppe kann gemäß Erwägungsgrund 48 als ein „berechtigtes Interesse“ gelten. Das kann man als „kleines Konzernprivileg“ deuten. Wenn eine Unternehmensgruppe dieses „Privileg“ nutzen will, so hat sie gewisse Anforderungen zu erfüllen.

➔ Ein Überblick über alle Arten des Daten-Transfers findet auf Seite 530.

In der **Fachliteratur** (siehe Seite 518) gibt es hilfreiche Dokumente: ● Die ZD 03/2021 berichtet auf Seite140-145 über zwei Alternativen zur Konzern-Auftragsverarbeitung: Eine „Controller-to-Controller-Übermittlung“ oder eine „gemeinsame Verantwortlichkeit“. ● Die 38-seitige GDD-Praxishilfe DS-GVO XVII („Mitarbeiterdaten im Unternehmensverbund“) liefert ausführliche Informationen.

13.8.1 Was ist eine Unternehmensgruppe?

Dieser Begriff ist in Artikel 4 Nr. 19 definiert: „*eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht*“. Details dazu finden sich im Erwägungsgrund 37.

Gemäß Erwägungsgrund 36 gilt der Hauptsitz des „herrschenden Unternehmens“ als der Hauptsitz der ganzen Unternehmensgruppe. Das hat Auswirkungen auf die zuständige Aufsichtsbehörde (und auf die Anwendung von ggf. vorhandenen nationalen Datenschutzgesetzen).

[Im Rahmen von PrivazyPlan® wird das Dossier „Unternehmensgruppe (Konzernprivileg)“ 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.]

13.8.2 Das berechtigte Übermittlungs-Interesse

Die Aussage von Erwägungsgrund 48 klingt zunächst unspektakulär:

> *„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind **können ein berechtigtes Interesse haben**, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, **zu übermitteln**.“*

Die DS-GVO sieht in der Unternehmensgruppe allerdings keinen gemeinsamen Verantwortlichen. Vielmehr bleibt jedes einzelne Unternehmen ein separater Verantwortlicher. Daher ist der Austausch von Daten in der Unternehmensgruppe als eine „**Übermittlung**“ anzusehen (siehe Kapitel 13.5 auf Seite 530).

Die Übermittlung ist ein Verarbeitungsvorgang gemäß Artikel 4 Nr. 2 und bedarf daher immer einer konkreten Rechtsgrundlage (Gesetz, Vertrag, Einwilligung, berechtigtes Geschäftsinteresse etc.) wie die Pflicht **[GVO_006]** auf Seite 121 ausführt.

Genau hier kommt das im Erwägungsgrund 48 erwähnte „berechtigte Interesse“ ins Spiel: Für die Rechtmäßigkeit der Verarbeitung bedarf es demnach in vielen Fällen eben KEIN Gesetz, Vertrag oder Einwilligung, weil auch das „berechtigte Interesse“ im Sinne des Artikel 6 (1f) eine Rechtsgrundlage darstellt.

Wenn eine Interessenabwägung zum Ergebnis kommt, dass die betroffenen Personen keine überwiegenden schützenswerten Interessen haben, dann ist die Übermittlung innerhalb der Unternehmensgruppe zulässig.

Der **eigentliche Nutzen** des Erwägungsgrund 48 liegt darin: In der Vergangenheit (also bis zum 25.05.2018) war es häufig nicht klar, wann ein Unternehmen ein berechtigtes Übermittlungs-Interesse hat.
Beispielsweise bei den Beschäftigtendaten gab es den Konsens, dass Arbeitsverträge einen eindeutig unternehmensübergreifenden Schwerpunkt haben mussten, damit die Übermittlung zwischen Unternehmen als „berechtigt“ angesehen werden könnte (z.B. beim Konzern-Vertriebsleiter).

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.9 Verschlüsselung

Fachinformationen

13.9.1 Unterliegen verschlüsselte Daten dem Datenschutz?

Verschlüsselung

Es ist eine der Kardinalfragen im Datenschutz: Unterliegen verschlüsselte Daten dem Datenschutz und somit den Bestimmungen der DS-GVO? Diese Frage sollte möglichst früh geklärt werden (siehe Seite 18).

Von dieser Antwort hängt beispielsweise ab,

- ob die sehr aufwändigen Verträge hinsichtlich einer Auftragsverarbeitungen gemäß Artikel 28 erforderlich sind, wenn die zu verarbeiteten Daten komplett verschlüsselt sind
- wie hoch die IT-Schutzmaßnahmen gemäß Artikel 32 ausfallen müssen, wenn z.B. ein USB-Stick verschlüsselt ist (darf man ihn in der Hosentasche tragen?)
- ob der Verlust von verschlüsselten Daten eine Datenschutzverletzung gemäß Artikel 33 darstellt, siehe Pflicht **[GVO_033]** auf Seite 170.

Leider besteht in dieser so wichtigen Frage keine Klarheit unter Datenschützern (siehe Kapitel 9.2.4 im TOM-Guide®, wo die verschiedenen Meinungen ausführlich dargestellt werden). Auch die DS-GVO nimmt hierzu leider keine konkrete Stellung.

Fachliteratur: • Zur Datenverletzungsmeldepflicht das WP-250 im Februar 2018 • Ausführliche Erörterungen im Januar 2018 hier. • Zu Anonymisierungstechniken im WP-216 dort auf Seite 35-36 im April 2014 (Verschlüsselung sei keine Anonymisierung). • Zur Meldepflicht im WP-213 im März 2014 (dort wird auf Site 10 der Verlust eines verschlüsselten Notebooks nicht als unbefugte Offenlegung angesehen, wohingegen dort in der Einleitung auf Seite 3 das Gegenteil behauptet wird).

[Im Rahmen von PrivazyPlan® wird das Dossier „Verschlüsselung“ (4 Treffer) und das Dossier „Pseudonymisierung“ (12 Treffer) und das Dossier „Anonymisierung“ (11 Treffer) 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.]

a) Ganz generell: Wann sind Daten personenbezogen?

Wann sind Daten objektiv auf eine Person bezogen, sodass gemäß Artikel 2 (1) und Artikel 4 (Nr. 1) der Datenschutz gilt? [166]

NICHT personenbezogen sind beispielsweise statistische Kennzahlen („heute sind 10 Beschäftigte erkrankt“) und Geschäftsdaten („die Maier AG hat einen Jahresumsatz von 1 Mio. Euro“) und anonymisierte Daten (also letztlich Buchstaben- und Zahlensalat).

KLAR personenbezogen sind die Stammdaten von Beschäftigten (Name, Adresse, E-Mail-Adresse, ..) und namentlich bekannter Kunden. Auch der Umgang mit E-Mails umfasst meist personenbezogene Daten (wegen namentlich genannter Adressaten und Absender).

ÜBERRASCHEND personenbezogen sind beispielsweise IP-Adressen (diese oftmals täglich ändernde Adresse (z.B. „85.107.455.16“) kann auf rechtlichem Wege durchaus dem Inhaber des Internet-Anschlusses zugeordnet werden). Interessanterweise sind z.B. auch die Geschäftsdaten von Freelancern, Kleingewerbetreibenden und Ein-Mann-GmbHs personenbezogen, weil sich diese Daten in letzter Konsequenz immer auf eine konkrete Person beziehen.

[166] Der Artikel 2 (1) zielt auf den Aspekte der **(teil-) automatisierten Verarbeitung** ab. Dies wird auf Seite 505 ausführlichst erläutert.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.10 Identifizierung einer betroffenen Person

Fachinformationen

Wie identifiziert (bzw. authentifiziert) man eine Person, die Auskunft oder sogar eine Daten-Kopien verlangt?
Keinesfalls darf man personenbezogene Daten an Betrüger aushändigen, weil sonst eine „Verletzung des Schutzes personenbezogener Daten“ vorläge (siehe Seite 157).

In der **Fachliteratur** (siehe Seite 518) gibt es viele hilfreiche Dokumente:
- 34. Jahresbericht der Aufsichtsbehörde Baden-Württemberg auf Seite 16-20
- DuD 02/2019 Seite 71-75 (verschiedene Identifikations-Methoden werden diskutiert).

⚠ Die unzureichende Identifizierung betroffener Personen hat im Dezember 2019 ein **Bußgeld** von (ursprünglich) fast 10 Mio. Euro nach sich gezogen, weil Kunden beim Telefonsupport nicht ausreichend sicher identifiziert wurden (es wurde nur der Name und das Geburtsdatum abgefragt). Das beschuldigte Unternehmen war kooperativ, aber das konnte das Bußgeld nicht verhindern. Der Vorwurf lautete: Die technisch-organisatorischen Maßnahmen waren nicht ausreichend (siehe Pflicht **[GVO_032]** auf Seite 158). Das LG Bonn hat das Bußgeld auf 900.000 € reduziert (siehe Seite 581).

➔ Es empfiehlt sich eine unternehmensweite **Richtlinie** zur sicheren Identifizierung betroffener Personen (siehe Seite 433). Dort können **(a)** die Beschäftigten allgemein sensibilisiert werden und **(b)** konkrete Vorgaben gemacht werden.

[Im Rahmen des PrivazyPlan® wird das Dossier „Identifizierung“ (ca. 13 Treffer) 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.]

13.10.1 Beispiele für notwendige Identifizierungen

Identifizierung einer betroffenen Person

Die folgenden Beispiele zeigen auf, wo eine Identifizierung notwendig sein kann:

- Die **Persönlichkeitsrechte** gemäß Artikel 13 bis Artikel 22 ermöglichen Auskünfte, Löschungen, Datenkopien und vieles mehr (siehe Seite 38). Bei zahlreichen Pflichten muss der Verantwortliche möglicherweise eine Identifizierung vorsehen. Siehe u.a. die Pflicht **[GVO_015a]** zur Datenkopie und die Pflicht **[GVO_020]** zur Datenübertragbarkeit.

- **Widerruf** von Einwilligung gemäß Artikel 7 (3): Theoretisch könnte ein Betrüger versuchen die Einwilligung einer Person vorzugaukeln. Siehe Pflicht **[GVO_007b]** auf Seite 148.

- **Einwilligungen durch die Eltern** gemäß Artikel 8 (2): Hier könnten die Kinder eine Einwilligung der Eltern vorgaukeln. Siehe Pflicht **[GVO_008]** auf Seite 155.

- **Datenschutzverletzung** an die betroffene Person melden gemäß Artikel 34 (1): Bevor die Details genannt werden, muss sichergestellt werden, das man wirklich mit der betroffenen Person kommuniziert. Siehe Pflicht **[GVO_034]** auf Seite 174.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.11 Geldbußen, Schadenersatz, Freiheitsstrafen (etc.)

Fachinformationen

Die DS-GVO findet weltweit Beachtung, weil die Gefahr von Schadenersatzforderungen und hohen Geldbußen enorm ansteigt. Dies soll hier thematisiert werden.

➔ Nähere Informationen zu den Aufsichtsbehörden finden sich auf Seite 595.

13.11.1 In Kurzform: Was droht bei Zuwiderhandlung?

Geldbußen, Schadenersatz, Freiheitsstrafen (etc.)

Manche Unternehmen könnten angesichts der Komplexität und des Umfangs der datenschutzrechtlichen Pflichten kapitulieren. Dies kann verschiedene Folgen nach sich ziehen:

Seitens der betroffenen Personen drohen:

- **Beschwerden.** Betroffene Personen könnten sich gemäß Artikel 77 bei der Aufsichtsbehörde beschweren. Da die Aufsichtsbehörden zu einer Reaktion gezwungen sind, wird das Unternehmen mit unangenehmen Fragebögen rechnen müssen. Viele deutsche Aufsichtsbehörden stellen Online-Beschwerdeformulare zur Verfügung (das senkt die Hemmschwelle erheblich).
  Der Erfahrung nach kümmern sich die Aufsichtsbehörden nicht nur isoliert um die konkrete Beschwerde, sondern fragen direkt auch andere Sachverhalte ab („Haben Sie einen Datenschutzbeauftragten bestellt?“, siehe den bayerischen Fragebogen vom Mai 2017).
  ➔ Ein Formular auf Seite 445 hilft beim Umgang mit Beschwerden.

- **Schadenersatz.** Die betroffenen Personen können gemäß Artikel 82 einen Schadenersatz fordern (siehe Seite 582). Dies gilt gleichermaßen für materielle und immaterielle Schäden. Die Beweislast liegt bei der betroffenen Person.
  Im Falle einer „gemeinsamen Verantwortlichkeit“ gemäß der Pflicht **[GVO_026]** auf Seite 192 gilt eine gesamtschuldnerische Haftung für alle Unternehmen, die an der Datenverarbeitung beteiligt sind.

- **Antrag auf Freiheitsstrafe.** Die betroffene Person kann gemäß § 42 BDSG bei der Staatsanwaltschaft eine Straftat anzeigen, durch die der Verantwortliche mit bis zu drei Jahren Freiheitsstrafe bestraft werden kann.

- **Unterlassungsansprüche durch die betroffene Person.** Eine betroffene Person kann eine Unterlassung fordern und dies auch gerichtlich durchsetzen (siehe Seite 591).

- **Gerichtliche Auseinandersetzungen.** Insbesondere gekündigte Mitarbeiter ziehen gerne vor Gericht, um den Ex-Arbeitgeber zu Auskünften (bzw. Daten-Kopien) und Löschungen zu zwingen. Das kostet den Arbeitgeber Nerven, Zeit und Geld. Der Streitwert einer Auskunft liegt wohl meist bei 500 €.

Seitens der Aufsichtsbehörden drohen:

- **Auflagen.** Die Aufsichtsbehörde kann auch konkrete Auflagen verhängen, die vom Unternehmen in einem gewissen Zeitraum eingehalten werden müssen (gemäß Artikel 58 (2d)).

- **Untersagungen.** Die Aufsichtsbehörde kann gemäß Artikel 58 (2f) bzw. Erwägungsgrund 94 eine Datenverarbeitung untersagen. Das Unternehmen darf diese Verarbeitung also nicht durchführen! Sollte diese Datenverarbeitung von elementarer Wichtigkeit sein, so könnte die Untersagung z.B. die Kundenbeziehung schwerwiegend beeinträchtigen.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.12 Ticket-System und Dokumenten-Managementsystem

Fachinformationen

Im Rahmen der Compliance-Anforderungen der DS-GVO (siehe Seite 502) gibt es viele neue Vorgänge und Dokumente.

Wie kann der Verantwortliche dabei den Überblick behalten?

13.12.1 Ticket-System für Datenschutz-Anliegen

Ein Ticket-System hilft bei der systematischen Bearbeitung von Kundenanliegen (siehe „Issue-Tracking-System“ bei Wikipedia). Im Grunde genommen handelt es sich um ein komplexes Aufgaben-Managementsystem.

Meist wird mittels eines Webbrowsers für jedes Anliegen ein „Ticket“ erstellt und bestimmten Mitarbeitern zugeordnet. Diese können das Ticket annehmen oder an andere Kollegen weiterleiten. Der dann zuständige Bearbeiter kann das Anliegen bearbeiten und mittels einer E-Mail-Anbindung im Rahmen dieses Tickets mit anderen Personen kommunizieren. Wenn das Anliegen erfüllt ist, wird das Ticket schlussendlich geschlossen. Sollte der Mitarbeiter zwischenzeitlich erkranken oder im Urlaub sein, so können andere Kollegen seine Tickets übernehmen. Der Status der Tickets (inklusive der Zeitüberschreitungen) ist jederzeit transparent ersichtlich. Im Nachhinein lassen sich Auswertungen erstellen, die die Anzahl und die Bearbeitungszeit der Tickets ausweisen; das ist im Rahmen der PDCA-Zyklen für die kontinuierliche Qualitätsverbesserung sehr hilfreich.

Im Rahmen der DS-GVO haben die betroffenen Personen zahlreiche Rechte, die der Verantwortliche teilweise in sehr knappen Zeiträumen erfüllen muss. Im Rahmen von PrivazyPlan® wurden mindestens 16 Pflichten identifiziert, wo ein Ticket-System sehr hilfreich sein kann (siehe Seite 593).

Hierzu ein Beispiel: Eine betroffene Person meldet sich am 01.06.2018 beim Unternehmen, um gemäß Artikel 15 (3) eine **Kopie ihrer Daten** zu erhalten. Im Rahmen von PrivazyPlan® ist dies die Pflicht [GVO_015a]. Nun hat das Unternehmen gemäß Artikel 12 (3) **einen Monat** Zeit, um diese Daten zu liefern (siehe Seite 39).

Ein Verstoß gegen diese Pflicht kann gemäß Artikel 83 (5b) eine Geldbuße von bis zu 20 Mio. Euro nach sich ziehen (siehe Seite 575). Für so ein Szenario ist ein Ticket-System perfekt geeignet.

Viele Unternehmen verfügen bereits über ein Ticket-System für die Belange der IT-Abteilung; hier können die Kollegen Probleme melden oder Hardware bzw. Zugriffsrechte anfordern. Auf solch einem System könnte ein Datenschutz-Ticketsystem sehr gut aufbauen.

Primär wird solch ein Datenschutz-Ticket-System im Unternehmen selbst genutzt. Im Einzelfall könnten Tickets aber durchaus auch vom Datenschutzbeauftragten erfüllt werden: Immer, wenn die betroffenen Personen oder die Aufsichtsbehörden Kontakt aufnehmen wollen, so dient der Datenschutzbeauftragte als Anlaufstelle. Sofern dies im Rahmen des Ticket-Systems erfasst werden soll, so muss auch der externe Datenschutzbeauftragte einen Zugriff auf den Ticket-Server erhalten.

Welches Ticketsystem ist empfehlenswert? Hier kann aufgrund der großen Produktvielfalt leider keine Empfehlung gegeben werden. Im Wikipedia-Artikel „Issue-Tracking-System“ werden zahlreiche Produkte genannt.
Diejenigen Unternehmen, die MS-Office nutzen, können die App „*Problemverfolgung*“ nutzen; mit wenigen Klicks lässt sich dieses Ticket-System auf Datenschutz-Belange anpassen.

Es gilt aber zu bedenken, dass in diesem Ticket-System auch personenbezogene Daten verarbeitet werden; sofern der Ticket-Server bei einem externen Unternehmen gehostet wird, so liegt gemäß Artikel 28 eine Auftragsverarbeitung vor. Dies muss zuvor vertraglich abgesichert werden.

Fazit: In Hinblick auf „Datenschutz-Compliance“ (siehe Seite 502) ist ein Ticket-System extrem hilfreich, wenn nicht sogar unverzichtbar. Durch PrivazyPlan® sind ca. 16 mögliche Ticket-Typen definiert, die man konkret umsetzen kann.

Es lassen sich Geldbußen entweder komplett vermeiden oder zumindest im Sinne des Artikel 83 (2) reduzieren, weil das Unternehmen sein Bemühen und seine Ernsthaftigkeit nachweisen kann (siehe Seite 575).

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.13 Aufsichtsbehörden / EU-Gremien

Fachinformationen

➔ Die **Sanktions-Möglichkeiten** der Aufsichtsbehörden (Bußgelder etc.) werden auf Seite 575 beschrieben.

Die personelle und finanzielle Ausstattung der europäischen Datenschutz-Aufsichtsbehörden ist wohl alles andere als ausreichend. In Brüssel liegt eine diesbezügliche Beschwerde (außer gegen Deutschland!) vor.

13.13.1 Deutsche Aufsichtsbehörden

In Deutschland gibt es 17 Datenschutz-Aufsichtsbehörden (eine Bundes- und 16 Landes-Aufsichtsbehörden). Alle Aufsichtsbehörden stellen **Online-Meldeformulare** zur Verfügung hinsichtlich Datenschutzverletzungen, Beschwerden, DSB-Meldungen etc. Für den PrivazyPlan® haben wir eine Liste aller Aufsichtsbehörden mitsamt aller ihrer Online-Formulare erstellt: www.privazyplan.eu/bundeslaender.htm.

Manche Aufsichtsbehörden in Deutschland sind hoffnungslos überlastet. Allein im öffentlichen Bereich sind in den ersten vier Monaten 11.000 Beschwerden und 6.100 Datenschutzverletzungen gemeldet worden; EU-weit waren es 55.000 Beschwerden und 18.900 Datenschutzverletzungen (aus dem Zahlenverhältnis wird klar, dass die Deutschen besonders viele Meldungen tätigen). In Portugal gehen die Bußgelder wohl auf das Konto der Aufsichtsbehörde und helfen bei der Schaffung neuer Arbeitsplätze.

Die ZD 04/2019 berichtet auf Seite XIV: In Deutschland sind seit Mai 2018 ca. 27.000 Beschwerden und 12.000 Datenschutzverletzungen eingegangen. In ganz Europa waren es 95.000 Beschwerden.

Die jährlichen Tätigkeitsberichte der Aufsichtsbehörden werden unter https://www.zaftda.de veröffentlicht (ab März 2019 übernimmt dies die „Stiftung Datenschutz“ und sorgt hoffentlich für mehr Kontinuität).

Im Dezember 2019 verhängte der Bundesdatenschutzbeauftragte (BfDI) ein Bußgeld über 10 Mio. Euro wegen mangelnder technisch-organisatorischer Maßnahmen. Betroffen war ein privatwirtschaftliches Telekommunikations-Unternehmen, welches unter die Aufsicht des BfDI fällt (siehe Seite 566).

➔ Die Interventionsmöglichkeiten finden sich z.B. auf Seite 589.

a) Die Datenschutz-Konferenz

Die Landesdatenschutz-Aufsichtsbehörden koordinieren sich miteinander in der sogenannten „**Datenschutz-Konferenz**“.

Die Funktionsweise dieses Gremiums ist für Außenstehende nicht ersichtlich. Der Vorsitz ändert sich ständig. Siehe https://www.datenschutzkonferenz-online.de.

Die Datenschutz-Konferenz ist ein wichtiges Gremium, weil sie u.a. Entschlüsse fasst, die sich früher oder später auf die behördliche Praxis auswirken. Leider ist es reine Glückssache, ob die Entschlüsse oder Positionspapiere auf den Websites veröffentlicht werden (ein besonderes prominentes Beispiel ist das Positionspapier zur Anwendbarkeit des Telemediengesetzes). Die derzeit zuverlässigste Quelle aller Entschließungen, Beschlüsse und Positionspapiere liefert der Bundes-Datenschutzbeauftragte hier.

Im Rahmen des PrivazyPlan® finden Sie die Dokumente ebenfalls aktuell (und teilweise kommentiert) hier.

b) Der Düsseldorfer Kreis

Seit 2013 dient dieses Gremium zur Abstimmung der Landesdatenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich. Die Aktivitäten dieses Gremiums sind wohl seit dem Jahr 2016 eher in die Datenschutz-Konferenz übergegangen (siehe oben).

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.14 Datenminimierung

Fachinformationen

Die Datenminimierung ist ein wichtiges Mittel in der DS-GVO. Das Ziel liegt darin, den Personenbezug (siehe Seite 556) zu minimieren oder sogar zu vermeiden.

➔ Siehe Artikel 5 (1c) und Pflicht **[GVO_005]** auf Seite 102. Dort wird u.a. auch eine Dokumentation hinsichtlich der Maßnahmen zur Anonymisierung bzw. Pseudonymisierung gefordert: „*Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)*“

➔ Siehe Artikel 25 (1) und Pflicht **[GVO_025]** auf Seite 106 zum Thema „Datenschutzfreundliche Technikgestaltung und Voreinstellungen [GVO_025]“.

Die im Folgenden genannten Maßnahmen kann der Verantwortliche nach freiem Ermessen gestalten; keinesfalls kann eine betroffene Person spezifische Maßnahmen zur Datenminimierung im Sinne des Artikel 5 (1c) verlangen (siehe Seite 161).

[Bei den Verantwortlichen, die mittels DSB-MIT-SYSTEM® betreut werden, wird der Aspekt der „Datenminimierung“ im Stammblatt einer jeden Verarbeitung thematisiert (siehe Seite 411), indem auf die Pflicht **[GVO_025]** verwiesen wird.]

Welche Maßnahmen sind angeraten?

13.14.1 Von Anfang an wenig Daten speichern

Im ersten Schritt geht es darum, dass schon zu Beginn möglichst wenig Daten gespeichert werden:

- Die Anzahl der von der Speicherung betroffenen Personen sollte auf das unbedingt Notwendige reduziert werden.
- Bei der Datenerhebung sollten möglichst viele Datenfelder auf freiwilliger Basis beruhen. Je weniger Pflichtfelder es gibt, desto besser.
- Datenschutzfreundliche **Technikgestaltung** und Voreinstellungen werden vom Artikel 25 (1) gefordert.

13.14.2 Daten möglichst „unscharf“ speichern

Je unpräziser die Daten sind, desto weniger Informationsgehalt haben sie, und desto weniger Schaden können sie im Ernstfall anrichten:

- Statt des genauen Körpergewichts eine Klassifizierung im Sinne von „70-75 Kg“.
- Statt eines genauen Zeitstempels speichert man nur das Datum (und lässt somit die Uhrzeit weg).
- Die IP-Adressen von Computern können gekürzt werden (z.B. 201.88.135.xxx)
- Manchmal reicht auch nur ein „ja/nein“ anstelle einer detaillierten Information.
- In manchen Fällen wäre sogar ein absichtliches „Verrauschen“ der Daten denkbar.
- Daten können durch Hashwerte ersetzt werden und sind somit nicht mehr im Klartext lesbar (siehe Kapitel 2.4.13 im TOM-Guide®).
- Jede Form von Verschlüsselung verhindert unbefugten den Zugriff auf die Daten (siehe Seite 556 und Kapitel 11.1 im TOM-Guide®), wodurch die Anzahl der gefährdeten Daten minimiert wird.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.15 Vereinfachte Risikoanalyse gemäß „Ulmer Modell“

Fachinformationen

Die DS-GVO scheint mit der Datenschutz-Folgenabschätzung gemäß Artikel 35 auf eine zweistufige Prüfung abzuzielen (siehe Pflicht **[GVO_035]** auf Seite 182).

Dies passt sehr gut zu der vereinfachten Risikoanalyse gemäß „Ulmer Modell“.[187], [188]

Vermutlich ist das Verarbeitungsverzeichnis ein guter Ort, um diese Risikoanalyse zu dokumentieren. Grob gesagt sieht diese „vereinfachte Risikoanalyse“ wie folgt aus:

13.15.1 Systemanalyse

In dieser ersten Stufe werden alle wesentlichen Geschäftsmodelle ermittelt. Dabei sind Systeme, Anwendungen, Daten und Personal zu berücksichtigen. In weiten Teilen könnte das Verarbeitungsverzeichnis (gemäß Artikel 30) diese Aufgabe erfüllen.

Was sind die typischen Systeme? Dies können – in Bezug auf die fragliche Verarbeitung – sein:

- Papierunterlagen bzw. Akten
- Lokale Computer, Notebooks, Mobile Devices, Smartwatch, USB-Stick, …
- Daten-Transfers: WLAN, mobiles Internet, Post, Paketdienst
- Websites (eigene oder fremde) und Webdienste und FTP-Server
- Externe Daten-Empfänger (Übermittlung, Auftragsverarbeitung oder gemeinsam Verantwortliche)
- …

Warum ist die „System-Analyse“ der erste Schritt? Weil Sie hier erkennen, wo überall ein Risiko drohen könnte. Nur mit Hilfe der Liste der Systeme können Sie sich gezielte Überlegungen zu den Risiken machen ohne etwas Wichtiges (z.B. die Website) zu übersehen.

Übrigens: Falls Sie ein Informations-Sicherheits-Managementsystem (ISMS, siehe Seite 524) eingerichtet haben, so wird es dort bestimmt schon eine Liste der Systeme geben. Diese können Sie dann hier wunderbar verwenden. Siehe Pflicht **[GVO_032]** auf Seite 158.

13.15.2 Ermittlung des Schutzbedarfs (Risikopotential)

Datenschützer sind sich dahingehend einig, dass der Umgang mit personenbezogenen Daten IMMER ein gewisses Risiko für die Rechte und Freiheit der betroffenen Personen bedeutet. Daher wird vom Verantwortlichen ~~Datenschutzbeauftragten~~ für jedes Verfahren abgeschätzt, wie hoch der maximal zu erwartende Schutzbedarf sein kann.
Die hierfür notwendigen Erkennungsmerkmale wurden oben bereits beschrieben. Wenn also z.B. sehr viele Personen betroffen sind und/oder sensible Daten verarbeitet werden und/oder eine intensive Überwachung stattfindet, dann hat das Verfahren einen **erhöhten Schutzbedarf**. Derzeit gibt es noch keinen praktikablen Ansatz, wo genau die Grenze eines erhöhten Schutzbedarfs verläuft.
Im Ergebnis kommt der Verantwortliche mit dieser Schutzbedarfs-Ermittlung seiner Pflicht gemäß Artikel 35 (2) nach, um „voraussichtlich hohe Risiken“ gemäß Artikel 35 (1) zu identifizieren.

Beispiel: Eine Online-Apotheke speichert beim Login die Benutzernamen und Passwörter von tausenden Kunden. Sollten diese Daten in unbefugte Hände

[Ab hier eine Lücke aufgrund der Leseprobe...]

[187] Siehe „Verfahrensverzeichnis 2.0“ von Markus Schäffter, Seite 74-77
[188] Siehe „Prozess zur Auswahl angemessener Sicherungsmaßnahmen“ (ZAWAS) der Datenschutz-Aufsichtsbehörde Niedersachsen. Siehe Datenschutz-PRAXIS 03/2019 Seite 6-9. Die Firma Althammer&Kill berichtet im Februar 2021, dass diese Erprobungsversion vom 30.11.2018 wohl überarbeitet wurde und irgendwann öffentlich publiziert wird. Diese 31-seitige PPT-Präsentation ist allerdings auch nicht gerade ein Praxisleitfaden; insbesondere der neuralgische Punkt der Risikoeinschätzung wird dort nur sehr kurz skizziert.

13.16 Allgemeines zur DS-GVO

Fachinformationen

Die meisten Unternehmen dürften nicht mit EU-Verordnungen vertraut sein. Daher soll im Folgenden eine kurze Einleitung in verschiedene Aspekte dieses Rechts erfolgen.

13.16.1 Warum der Name „Grund“-Verordnung?

Allgemeines zur DS-GVO

Parallel zur hier im PrivazyPlan® thematisierten (Grund-) Verordnung (EU) 2016/679 gibt es auch noch die Richtlinie (EU) 2016/680 speziell für Behörden im Zusammenhang mit Strafverfolgung und Strafvollzug (siehe Seite 262).

Insofern regelt die Grundverordnung „nur“ die grundlegenden Dinge (daher der Name).

13.16.2 Eine EU-Verordnung ist unmittelbar gültig

Allgemeines zur DS-GVO

Wenn Brüssel eine „Verordnung“ (engl. „regulation“) beschließt, dann ist diese unmittelbar in ganz Europa rechtlich wirksam. Es bedarf keiner weiteren Beschlüsse in den nationalen Parlamenten.

Dies unterscheidet die Verordnung von einer „Richtlinie“ (engl. „directive“), die immer von allen nationalen Parlamenten in jeweils nationales Recht umgesetzt werden muss.

Zu einer Verordnung greift Brüssel immer dann, wenn ein rechtlicher Rahmen nicht durch nationale Parlamente „verwässert“ werden soll. Dies war bei der EU-Datenschutz-Richtlinie 95/46/EG von 1995 der Fall, wo insbesondere die irische Aufsichtsbehörde im Zusammenhang mit großen US-Internet-Diensteanbietern in ganz Europa für Unmut gesorgt hatte.

Gemäß Artikel 99 ist die DS-GVO ist im Mai 2016 in Kraft getreten. Am **25.05.2018** endet die Umsetzungsfrist. Ab dann müssen alle Pflichten erfüllt sein. Gemäß Artikel 94 ist die EU-Richtlinie von 1995 aufgehoben.

13.16.3 Öffnungsklauseln

Allgemeines zur DS-GVO

An dutzenden Stellen ermöglicht die DS-GVO den nationalen Parlamenten eine Anpassung an nationale Rechtsvorschriften (siehe auch Seite 263).

In Deutschland wurde diese Chance ergriffen und im April 2017 unter höchstem zeitlichen Druck ein inhaltlich stark umstrittenes neues Bundesdatenschutzgesetz beschlossen (siehe Seite 278).

Einerseits ist es sehr begrüßenswert, dass die nationalen Parlamente eine „Brücke“ zwischen der EU-Verordnung und nationalen Gesetzen schlagen dürfen. Andererseits wird die Rechtslage für den Anwender dadurch sehr unübersichtlich.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.17 Videoüberwachung / Fotografie

Fachinformationen

13.17.1 Videoüberwachung

Die Videoüberwachung wird in der DS-GVO eigentlich nicht besonders thematisiert. Sie ist somit eine Verarbeitung wie jede andere auch.

Das Dossier „Videoüberwachung“ zeigt die beiden Stellen, wo sich die DS-GVO auf dieses Thema bezieht. Weil aber die Videoüberwachung ein sehr wichtiges Thema ist, soll hier in diesem Kapitel speziell darauf eingegangen werden.

➔ Siehe die „weiche“ Pflicht [AUX_012] auf Seite 325.

Die **Fachliteratur** (siehe Seite 518) liefert verschiedene Hinweise: Fotos im geschäftlichen Bereich (und wie man sich dagegen wehrt) in Datenschutz-PRAXIS 12/2020 Seite 8-9 ● 41-seitige DSK-Orientierungshilfe im Juli 2020 ● 15-Punkte-Fragenkatalog der Aufsichtsbehörde Baden-Württemberg im Juni 2020 ● Die Datenschutz-PRAXIS 04/2020 Seite 8-11 liefert Checklisten und Infos ● EDPB-Guideline 2019-03 „Videosurveillance“ im Juli 2019 (auf Anfrage kann der Autor des PrivazyPlan® eine automatisierte deutsche Übersetzung liefern) ● 34. Jahresbericht der Aufsichtsbehörde Baden-Württemberg auf Seite 31-33 und hinsichtlich der Videoüberwachung am Arbeitsplatz auf Seite 38-42. ● Ausführliche Hinweise in der ULD-Praxisreihe 5 auf 17 Seiten. ● DSK-Kurzpapier-15 ● Fachzeitschrift ZD 09/2017 Seite 407-411.

a) Was ist die Rechtsgrundlage für Videoüberwachungen?

Jede Verarbeitung braucht eine Rechtsgrundlage, wie die Pflicht [GVO_006] ab Seite 122 beschreibt.

- Bei der Videoüberwachung öffentlich zugänglicher Bereiche wird in aller Regel das „berechtigte Interesse“ im Sinne des Artikel 6 (1f) zum Tragen kommen (siehe Seite 134).
  Das Bundesverwaltungsgericht hat im März 2019 entschieden, dass eine anlasslose Videoüberwachung in einer Zahnarztpraxis nicht rechtmäßig ist (Az. C 2.18, siehe auch hier). Es bedarf also (wie schon immer) konkreter Begründungen, warum eine Videoüberwachung erforderlich ist.
  Auch das OLG Stuttgart fordert konkrete und stichhaltige Begründungen für die Videoüberwachung im Supermarkt (Az. 12 U 296/20 vom 18.05.2021).

- Falls die Beschäftigten des Verantwortlichen betroffen sind, so kann der § 26 BDSG angewendet werden, sofern **(a)** eine entsprechende Betriebsvereinbarung abgeschlossen ist oder **(b)** der Arbeitsvertrag eine solche Videoüberwachung erfordert.

  Das Bundesarbeitsgericht hat entschieden, dass Videoüberwachungen auch nach vielen Monaten noch verwendet werden können, um Inventardifferenzen aufzuklären und die Beschäftigten wegen Diebstahl zu kündigen (Az. 2 AZR 133/18 vom 23.08.2018).

  Die Frage der Verwertbarkeit der Videoaufnahmen bei Diebstahl durch Beschäftigte ist nicht trivial und muss genau geprüft werden. Ein BAG-Urteil gibt den Arbeitgebern gewisse Freiheiten (Az. 8 AZR 421/17 vom 28.03.2019, siehe auch hier).

In Deutschland regelt zwar der § 4 BDSG den Umgang mit der Videoüberwachung, doch war sich die Fachwelt im April 2018 einig, dass der deutsche Gesetzgeber hier über **keine passende Öffnungsklausel** (siehe Seite 610 mit ausführlicher Erläuterung).
Die in Deutschland bisher übliche Unterteilung zwischen „öffentlich zugänglichen Bereichen“ und „internen Bereichen eines Unternehmens“ existiert nicht mehr. Alles folgt den gleichen Regeln.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.18 Verpflichtung auf Vertraulichkeit und Datengeheimnis

Fachinformationen

13.18.1 Was ist wirklich erforderlich? Was ist empfehlenswert?

Die **Verpflichtung auf Datengeheimnis und Vertraulichkeit** ist leider kein triviales Thema. In Deutschland war es bis zum 25.05.2018 im Rahmen des § 5 BDSG-alt ganz klar geregelt, dass sich alle Beschäftigten zum Datengeheimnis verpflichten müssen. So einfach ist es im Rahmen der DS-GVO leider nicht mehr.

Das Thema wäre auch zukünftig kein Problem, wenn nicht einzelne Beschäftigte (oder stellvertretend sogar der Betriebsrat) sich weigern würden, eine solche Verpflichtung zu unterzeichnen. Daher gilt es sehr sorgsam zu argumentieren, welche Maßnahmen absolut verpflichtend sind (und welche eher optional sind).

Nimmt man die DS-GVO wörtlich, so ist es nur gemäß Artikel 28 (3b) im Rahmen von **Auftragsverarbeitungen** erforderlich, dass sich die Beschäftigten zur Vertraulichkeit verpflichten (sofern sie nicht schon einer gesetzlichen Verschwiegenheitspflicht unterliegen).

> „*Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags [...] Dieser Vertrag sieht insbesondere vor, dass der Auftragsverarbeiter gewährleistet, dass* ***sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet*** *haben [...]*“

Fachlich gesehen ist es aber eigentlich absurd, dass eine Vertraulichkeits-Verpflichtung nur für die relevanten Beschäftigten von Auftragsverarbeitern gelten soll. Dementsprechend haben die deutschen Aufsichtsbehörden einhellig im DSK-Kurzpapier-19 formuliert:

> „*Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten“ sind, trifft inhaltlich diese „verpflichtende Unterrichtung“ (im Folgenden: Verpflichtung)* ***auch die Verantwortlichen und ihre Beschäftigten****. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und ggfls. der Aufsichtsbehörde nachweisen), ist nicht verbindlich geregelt. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen.*“

Auch die NRW-Aufsichtsbehörde schreibt in einer 40-seitigen Broschüre: „***Alle Personen*** *im Verein, die auf personenbezogene Daten zugreifen können, sollten schriftlich auf die Vertraulichkeit verpflichtet werden*“.

Mit anderen Worten: Wenn ein Verantwortlicher sich nur auf den reinen Wortlaut der DS-GVO verlässt (und nicht alle Beschäftigten verpflichtet), dann werden die Aufsichtsbehörden ihm ggf. ein Organisationsversagen vorwerfen. Das kann unangenehme Konsequenzen haben.

Nach einhelliger Einschätzung der Fachliteratur ist es jedoch ratsam, dass jeder Verantwortliche seine Beschäftigten auf Verschwiegenheit bzw. Vertraulichkeit verpflichtet. Sofern dieser Schritt im Rahmen des § 5 BDSG-alt bereits vorgenommen wurde, so ist eine Wiederholung wohl nicht unbedingt erforderlich.

Die Verschwiegenheits-Verpflichtung der Beschäftigten ist insbesondere wichtig für den „Nachweis der Einhaltung der Grundsätze (Accountability)“ im Rahmen der Pflicht **[GVO_005]** ab Seite 102.

Der Datenschutzbeauftragte unterliegt gemäß Artikel 38 (5) der Vertraulichkeit und muss diesbezüglich nicht zusätzlich schriftlich verpflichtet werden.

Der § 53 BDSG ist hier im PrivazyPlan® **irrelevant**, weil er im Teil 3 des BDSG angesiedelt ist (und somit nur für die Justiz und Strafverfolgung gilt).

Konkret welcher Wortlaut ist gefordert, wenn die DS-GVO von „*sich verpflichten*“ spricht? Reicht hier eine indirekte/passive Formulierung im Sinne von „*ich nehme zur Kenntnis, dass ich der Vertraulichkeit unterliege*“? Mitunter gibt es diesbezüglich Diskussionen.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.19 Website (Tracking / Cookies / Unterrichtung…)

Fachinformationen

Der Datenschutz auf der Website ist nach wie vor ein wichtiges und kontroverses Thema. Ab Juli 2019 wird hier im PrivazyPlan® ein neues Kapitel eröffnet, um die komplexen Zusammenhänge zu erklären.

Letztlich ist die „weiche“ Pflicht **[AUX_005]** betroffen („Grundlegende Anforderungen an Websites und Apps“), siehe Seite 321.

13.19.1 Begriffsbestimmungen

Website

Einige zentrale Begriffe hinsichtlich der Website werden hier kurz definiert und erläutert:

- **„Website“:** Hiermit ist beispielsweise der gesamte Inhalt von www.privazyplan.de gemeint (siehe Wikipedia).
  Im Gegensatz dazu meint der Begriff „**Webseite**“ eine konkrete Seite, wie z.B. www.privazyplan.de/demo.htm. Diese sprachliche Unterscheidung fehlt in vielen Fachbeiträgen. Und wenn die Datenschutz-Konferenz von „*webseitenübergreifenden Tracking*“ spricht, dann fragt man sich, was die Autoren damit genau meinten.
  Die Websites sind technologisch so ausgelegt, dass die zugrundeliegenden Webserver zunächst einmal „kein Gedächtnis“ über das Klickverhalten der Nutzer haben (sie sind „zustandslos“). Diese „Dummheit“ lässt sich u.a. mittels Cookies überwinden (siehe weiter unten).

  Vorsicht bei den **Website-Baukästen** mancher Internetprovider; für ca. 15 Euro monatlich soll eine Website schnell erstellt sein. Wir können vor diesen Produkten nur warnen, weil der Datenschutz dort meist keine große Rolle spielt. Die c't 19/2020 hat einige Produkte grob getestet, ohne über die eklatanten Missstände zu berichten (siehe Leserbrief von Nicholas Vollmer in c't 20/2020). Siehe Kapitel 6.7 in „Digitalisierung.docx“ in der PrivazyPlan.zip (siehe Seite 29).

- **„IP-Adresse“**: Jeder Nutzer erhält eine IP-Adresse, wenn er sich mit dem Internet verbindet. Derzeit ist die **IPv4**-Variante noch am verbreitetsten; sie hat das Muster „106.169.246.243“ und liefert somit maximal 4 Mrd. Möglichkeiten (32 Bit), die ganz bald erschöpft sind. Die allermeisten Menschen erhalten daher eine „**dynamische**“ IP-Adresse, die sich jede Nacht ändert. Dieser Zusammenhang ist datenschutzrechtlich wichtig, weil die IP-Adresse als personenbezogen gilt, wobei es aber recht schwierig ist herauszufinden, welche IP-Adresse eine natürliche Person gestern hatte. Nur Unternehmen erhalten eine „**statische**“ und somit dauerhaft identische IP-Adresse, wobei sich hier aber alle Mitarbeiter hinter der gleichen IP-Adresse verstecken und somit für den Website-Betreiber kaum zu identifizieren sind. Auf diese wichtigen Zusammenhänge wird leider nur sehr selten eingegangen.
  Hingegen wird es datenschutzmäßig brisant, wenn sich die **IPv6**-Adresse zukünftig durchsetzen werden. Mit einer enormen Länge von 128 Bit könnte letztlich fast jeder Sandkorn auf der Erde eine dauerhafte IP-Adresse bekommen. Spätestens dann ist jedes Verhalten dieser IP-Adresse hochgradig individualisiert und theoretisch dauerhaft nachvollziehbar. [197]

[197] Hoffentlich werden alle Geräte einen „Reset“-Knopf erhalten, der auf Wunsch des Nutzers eine neue IP-Adresse anfordert. Die Fritzbox beherrscht dieses Feature schon seit Langem. Damit wäre die Forderung nach „Datenminimierung“ erfüllt, siehe Pflicht **[GVO_025]** auf Seite 102.

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.20 Konsequente Digitalisierung (anlässlich Corona-Pandemie)

Fachinformationen

Seit Dezember 2019 hat das Virus SARS-CoV-2 die Welt zunehmend im Griff. Auch diese Pandemie ist – wie zuletzt im Jahr 2002 - auf ein SARS-Virus zurückzuführen. Im März 2020 ist Europa der Schwerpunkt der Pandemie und ist von weitgehende Konsequenzen betroffen: Grenzsperrungen, Einreiseverbote, Ausgangsverbote, häusliche Quarantäne und Homeoffice in den Unternehmen.

Die Menschen werden nun (zeitlich begrenzt) einen erhöhten räumlichen Abstand voneinander halten müssen. All dies hat auch Auswirkungen auf den Datenschutz, weil dieser räumliche Abstand durch digitale Mittel (VPN-Zugänge, Videokonferenzen, etc.) kompensiert werden muss.

Das langfristige Ergebnis wird eine **konsequente Digitalisierung** sein, und diese wird uns in den nächsten Jahren noch intensivst beschäftigen. Bei dieser Digitalisierung ist unbedingt auch der Datenschutz zu beachten, weil nur so die generelle Rechtmäßigkeit sichergestellt ist (und somit weder Zeit noch Geld verschwendet werden).

Die „**Digitale Transformation**“ ist schon lange ein Thema (siehe hier und hier) und wird durch das EuGH-Urteil zum Drittland-Datentransfer erheblich verkompliziert (siehe Seite 496). Entwickeln Sie rechtzeitig eine Digitale Strategie, um Ihr Unternehmen zu schützen (siehe Seite 658).

13.20.1 Digitalisierung der Unternehmen wird RAPIDE zunehmen

Konsequente Digitalisierung

Die zunehmende Digitalisierung der Wirtschaft war schon immer ein Thema, aber durch die Corona-Pandemie wird dies wahrlich explosionsartig intensiviert. Im März 2020 wurden wir alle insofern **um ein Jahrzehnt in die Zukunft geschleudert**. Das gilt für alle Unternehmen und auch für die öffentlichen Verwaltungen.

Die zunehmende Digitalisierung entspricht dem „Zeitgeist“ und wird deswegen rapide zunehmen. Insofern hat die sowieso bestehende Digitalisierung unseres (Arbeits-) Lebens nun einfach nur noch eine zusätzliche Raketen-Stufe hinzugewonnen.

Die Corona-Pandemie wird sich zu einem Kollektiven Trauma entwickeln. Auch wenn sie (hoffentlich bald) überstanden sein wird, so wird die Welt nicht mehr sein wie vorher.
Zukünftig werden Banken, Wirtschaftsprüfer und Berater für viele Jahre EINE ganz bestimmte Frage stellen: **Wie ist Ihr Unternehmen auf elementare Krisen (Epidemie, Nuklear-Katastrophe, Stromausfall und sogar Krieg) vorbereitet?** Die Antwort wird oftmals lauten: Durch konsequente Digitalisierung in all ihren Aspekten!

Spätestens im März 2020 sollte eines klar geworden sein: Wer sein Unternehmen nicht (belastbar!) digitalisiert, der hat in der nächsten Krise schlechte Chancen auf wirtschaftliches Überleben.

⚠ ACHTUNG: Die konsequente und belastbare Digitalisierung von Geschäftsprozessen stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz!
Ihr betrieblicher Datenschutzbeauftragter unterstützt Sie bei der zukunftssicheren Investition von Zeit und Geld.

a) Herausforderung der IT-Sicherheit

Hinsichtlich der IT-Sicherheit und der Corona-Pandemie bekommt der Artikel 32 plötzlich eine ganz andere Bedeutung: Der Verantwortliche trifft Maßnahmen, um **(a)** die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zu-

[Ab hier eine Lücke aufgrund der Leseprobe...]

13.21 Technisch-organisatorische Maßnahmen

Fachinformationen

Jedes Unternehmen trifft technisch-organisatorische Maßnahmen, um personenbezogene Daten zu schützen. Das ist die gute Nachricht.

Die getroffenen Maßnahmen werden aber meist unsystematisch und rein zufällig ausgewählt. Das ist die schlechte Nachricht.

Solange Sie keine Berührung mit einer Datenschutz-Aufsichtsbehörde haben und nicht wegen Schadenersatz verklagt werden (siehe Seite 582), ist das kein Problem. [212] Doch sobald Ihre technisch-organisatorischen Maßnahmen unter die Lupe genommen werden, könnte es ganz schnell kritisch werden. Insofern macht es Sinn, dass Sie sich rechtzeitig mit der systematischen Auswahl von technisch-organisatorischen Maßnahmen beschäftigen.

[212] Genau gesagt ist es kein Problem, solange man nicht die Rechte und Freiheiten der betroffenen Personen beeinträchtigt... und solange man keine Kundschaft verärgert oder sogar wertvolle Mitarbeiter/innen verliert... oder keinen Ärger mit dem Betriebsrat bekommt... oder als Auftragsverarbeiter keine Aufträge mehr bekommt... oder einen Datenverlust erleidet, der das ganze Unternehmen lahmlegt (z.B. durch Ransomware)... und die Cyberversicherung nicht zahlt, weil man sich nicht genügend geschützt hat.

13.21.1 Was sind technisch-organisatorische Maßnahmen?

Technisch-organisatorische Maßnahmen

An ca. 25 Stellen erwähnt die DS-GVO die sogenannten „technisch organisatorischen Maßnahmen“. Im Gegensatz zum alten BDSG und der Anlage zu § 9 BDSG-ALT gibt es aber keine klare Definition.

Im Grunde genommen geht es hier um Maßnahmen jeglicher Art, die sich in zwei Kategorien einteilen lassen:

- technische Maßnahmen, also die Konfiguration von **Maschinen** betreffend
- organisatorische Maßnahmen, also die **Menschen** betreffend.

Mit anderen Worten: Es geht um Maßnahmen jeglicher Art, insbesondere: **(a)** wie man Software konfiguriert, **(b)** wie man die Beschäftigten konkret anweist, **(c)** wie Gebäude, Computer und USB-Datenträger schützt, **(d)** wie man Zugriffsrechte auf Daten einschränkt.

Die DS-GVO erwähnt die technisch-organisatorischen Maßnahmen an ca. 25 Stellen derart inflationär, dass man sie begrifflich kaum zu fassen bekommt.

Letzten Endes geht es um alle Maßnahmen, die den Datenschutz fördern.

13.21.2 Worauf zielen die technisch-organisatorischen Maßnahmen ab?

Technisch-organisatorische Maßnahmen

Klassischerweise würde man diese Maßnahmen auf die üblichen technischen IT-Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit beziehen.

Doch die Reichweite dieser technisch-organisatorischen Maßnahmen **reicht viel weiter**, wie die folgende – keinesfalls vollständige – Liste zeigt:

- Schutz von Pseudonymen in Artikel 4 Nr. 5

[Ab hier eine Lücke aufgrund der Leseprobe...]

Eine Kurzzusammenfassung der Pflichten findet sich auf Seite 674; eine tabellarische Übersicht auf Seite 689.

Die Basis-Checklisten des PrivazyPlan® für einen schnellen thematischen Einstieg findet sich auf Seite 310.

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

Station 2: Liste der bußgeldbewehrten Pflichten

Welche Pflichten gibt es im Datenschutz? Dies ist der Dreh- und Angelpunkt des PrivazyPlan®. Es sind [sorry!] ca. 50 Pflichten, die man kennen und einhalten muss. Auf diesen ca. 11 Seiten ist alles kürzest möglich zusammengefasst. Bitte lesen Sie sich das unbedingt einmal durch.

< Zurück • Home • Weiter >

In den Kapiteln 2 bis 10 (auf den Seiten 38 bis 277) werden alle Pflichten des Verantwortlichen ausführlich beschrieben und angeleitet. Ein Klick auf den jeweiligen Absatz führt direkt nach oben in die Pflicht-Kapitel.

(NICHT aufgeführt werden hier die „weichen" Pflichten, die nicht bußgeldbewehrt sind. Diese „weichen" Pflichten sind eher als „Strategien" zu bezeichnen, und sind für einen erfolgreichen Datenschutz durchaus wichtig. Siehe Seite 319.)

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. ➔ Siehe Seite 39.

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 415). ● 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.

Zweckänderung vorab mitteilen [GVO_013a]

Gemäß Artikel 13 (3) bzw. Artikel 14 (4) muss die betroffene Person über geplante Zweckänderungen vorab informiert werden. Möglicherweise hat die betroffene Person ein Widerspruchsrecht, falls sie glaubt, dass ihre „Rechte und Freiheiten" unzulässig beschnitten werden. Die DS-GVO nennt diesen Vorgang auch „*Weiterverarbeitung*" (engl. „*further processing*"). ➔ Siehe Seite 46.

In aller Kürze geht es darum: ● Stellen Sie sicher, dass jede geplante Zweckänderung rechtzeitig erkannt wird. ● Prüfen Sie, ob bei einer geplanten Zweckänderung eine Vorab-Information an die betroffenen Personen notwendig ist. ● Erstellen Sie den geforderten Informationstext (sofern er nicht schon durch einen gemeinsamen „Transparenz"-Text erstellt wurde, siehe Seite 415). ● Führen Sie die Information durch (und weisen Sie auf die relevanten Änderungen hin). ● ➔ Nutzen Sie das Beispielformular von Seite 342, um eine betroffene Person zu informieren.

Bei Erhebung von Daten über Dritte informieren [GVO_014]

Gemäß Artikel 14 (1) und Artikel 14 (2) muss der Verantwortliche die betroffenen Personen darüber informieren, dass ihre Daten an anderer Stelle (also durch einen Dritten) erhoben wurden. Dies geschieht spätestens innerhalb von vier Wochen. Doch es gibt auch zahlreiche Ausnahmen. ➔ Siehe Seite 50.

In aller Kürze geht es darum: ● Besorgen Sie sich das Verarbeitungsverzeichnis, um alle betroffenen Verarbeitungen zu identifizieren, wo Daten durch Dritte erhoben werden. ● Erstellen Sie den geforderten Informationstext (sofern er nicht schon durch einen gemeinsamen „Transparenz"-Text erstellt wurde, siehe

[Ab hier eine Lücke aufgrund der Leseprobe...]

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 12).

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 12).
Wo können Sie die Arbeitsergebnisse speichern, wenn sie diese Pflichten erfüllen? Wir empfehlen die Verzeichnisstruktur der PrivazyPlan.zip auf Seite 29.

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)	40
2.2	Zweckänderung vorab mitteilen [GVO_013a]	Artikel 13 (3)	46
2.3	Bei Erhebung von Daten über Dritte informieren [GVO_014]	Artikel 14	50
2.4	Auskunft erteilen [GVO_015]	Artikel 15 (1,2)	55
2.5	Datenkopie aushändigen [GVO_015a]	Artikel 15 (3,4)	58
2.6	Berichtigung ermöglichen [GVO_016]	Artikel 16	70
2.7	Löschen aus betrieblichen Gründen [GVO_017]	Artikel 17 (1)	72
2.8	Löschen auf Verlangen der betroffenen Person [GVO_017a]	Artikel 17 (1)	75
2.9	Löschen veröffentlichter Daten („Recht auf Vergessenwerden“) [GVO_017b]	Artikel 17 (2)	77
2.10	Einschränkung der Verarbeitung [GVO_018]	Artikel 18	80
2.11	Korrektur bei Dritten (Nachberichtigung) [GVO_019]	Artikel 19	84
2.12	Datenübertragbarkeit ermöglichen [GVO_020]	Artikel 20	88
2.13	Widerspruchsrecht einräumen [GVO_021]	Artikel 21	93
2.14	Automatisierte Entscheidung vermeiden [GVO_022]	Artikel 22	97

Pflichten zu Dokumentationen und Nachweisen

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

3.1	Nachweis der Einhaltung der „Grundsätze“ [GVO_005]	Artikel 5 (2)	102
3.2	Datenschutzfreundliche Technikgestaltung und Voreinstellungen [GVO_025]	Artikel 25	106
3.3	Verarbeitungsverzeichnis des Verantwortlichen [GVO_030]	Artikel 30 (1)	110
3.4	Verarbeitungsverzeichnis des Auftragsverarbeiters [GVO_030a]	Artikel 30 (2)	116

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)	122
4.2	Zweckänderungen müssen sorgsam geprüft werden [GVO_006a]	Artikel 6 (4)	137
4.3	Einwilligungen müssen dauerhaft nachweisbar sein [GVO_007]	Artikel 7 (1)	142
4.4	Einwilligungstexte müssen klar erkennbar und gut verständlich sein [GVO_007a]	Artikel 7 (2)	146
4.5	Einwilligung muss jederzeit (und einfach) widerrufbar sein [GVO_007b]	Artikel 7 (3)	148
4.6	Die Freiwilligkeit von Einwilligungen muss unbestreitbar sein [GVO_007c]	Artikel 7 (4)	151
4.7	Einwilligungen von Kindern durch Eltern legitimieren [GVO_008]	Artikel 8 (2)	155

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)	158
5.2	Beschäftigte Personen sind konkret anzuweisen [GVO_032a]	Artikel 32 (4)	165
5.3	Datenschutzverletzungen dauerhaft dokumentieren [GVO_033]	Artikel 33 (5)	170
5.4	Datenschutzverletzungen an Aufsichtsbehörde melden [GVO_033a]	Artikel 33 (1)	174
5.5	Betroffene Person über Datenschutzverletzung benachrichtigen [GVO_034]	Artikel 34 (1)	178

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	182
6.2	Konsultation der Aufsichtsbehörde [GVO_036]	Artikel 36	189

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	192
7.2	EU-Vertreter benennen [GVO_027]	Artikel 27	204
7.3	Auftragsverarbeitung detailliert regeln [GVO_028]	Artikel 28	207
7.4	Auftragsverarbeitung streng nach Weisung durchführen [GVO_028a]	Artikel 28 (3a)	214
7.5	Auftragsdatenverarbeitung aus BDSG übernehmen [GVO_028b]	Artikel 28 (3)	220
7.6	Datentransfer an Drittländer ist stark reglementiert [GVO_044]	Artikel 44	222

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)	235
8.2	Bekanntmachung des Datenschutzbeauftragten [GVO_037a]	Artikel 37 (7)	242
8.3	Frühzeitige Einbindung des Datenschutzbeauftragten [GVO_038]	Artikel 38 (1)	245
8.4	Unterstützung des Datenschutzbeauftragten [GVO_038a]	Artikel 38 (2)	248
8.5	DSB als Anlaufstelle für betroffene Personen [GVO_038b]	Artikel 38 (4)	250
8.6	Unterrichtung und Beratung hinsichtlich der Pflichten [GVO_039]	Artikel 39 (1a)	252
8.7	Überwachung der Einhaltung von Datenschutzvorschriften [GVO_039a]	Artikel 39 (1b)	254
8.8	Anlaufstelle für Aufsichtsbehörde und Zusammenarbeit [GVO_039b]	Artikel 39 (1e)	257

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:

9.6.1	Berufliche Schweigepflicht [STGB_203]	§ 203 StGB	270
9.6.2	Unzumutbare Werbe-Belästigungen [UWG_007]	§ 7 UWG	271
9.6.3	Jugendschutz in Telemedien nicht kommerzialisieren [TTDSG_020]	§ 20 TTDSG	274
9.6.4	Privatsphäre im Webbrowser etc. [TTDSG_025]	§ 25 TTDSG	274

Pflichten durch das neue Bundesdatenschutzgesetz

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

~~10.1~~	~~OBSOLET: Videoüberwachungen kenntlich machen~~	~~§ 4 Abs. 2~~	~~280~~
~~10.2~~	~~OBSOLET: Identifizierte Personen von Videoüberwachung informieren [BDSG_004a]~~	~~§ 4 Abs. 4~~	~~281~~
10.3	Sicherheitsmaßnahmen bei sensiblen Daten [BDSG_022]	§ 22 Abs. 2	282
10.4	Sensible Forschungsdaten anonymisieren [BDSG_027]	§ 27 Abs. 3	284
10.5	Auskunftei muss EU-Darlehensgebern Auskunft geben [BDSG_030]	§ 30 Abs. 1	286
10.6	Abgelehnte Finanzierung muss Auskunftei als Grundlage nennen [BDSG_030a]	§ 30 Abs. 2	287
10.7	Verweigerung von Auskünften dokumentieren etc. [BDSG_034]	§ 34	288
10.8	Verarbeitungs-Einschränkung anstelle Löschung kommunizieren [BDSG_035]	§ 35 Abs. 2	290

„Weiche“ Pflichten (die nicht bußgeldbewehrt sind, sondern eher „Strategien“ darstellen)

Im Kapitel 12.1.7 wird eine Reihe von **Strategien** erwähnt, die der Datenschutzbeauftragte ebenfalls überwachen könnte.

1.) Beschäftige schulen und zur Vertraulichkeit verpflichten [AUX_001]	319
2.) Beschäftigte unterliegen einer Regelung zur Privatnutzung [AUX_002]	319
3.) Beschäftigte unterzeichnen EDV-Nutzungsvereinbarung [AUX_003]	320
4.) Datenschutz beim Betriebsrat regeln [AUX_004]	321
5.) Grundlegende Anforderungen an Websites und Apps [AUX_005]	321
6.) Erstellen und veröffentlichen von Fotos durch Journalisten [AUX_006]	322
7.) Stammblatt einer jeden Verarbeitung erzeugen [AUX_007]	322
8.) Stammblätter sind komplett bearbeitet [AUX_007a]	323
9.) Datenschutz-Managementsystem einrichten [AUX_008]	323
10.) Bring your own device (“BYOD”) [AUX_009]	323
11.) Lösch-Konzept (Akten, Datenträger, Löschverlangen) [AUX_010]	324
12.) Transparenztext einer jeden Verarbeitung erstellen [AUX_011]	324
13.) Korrekter Umgang mit Videoüberwachungen [AUX_012]	325

14.4 Unsichere Sachverhalte (rote Bomben)

Anhang

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

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

14.4.1 Pflichten aufgrund von Persönlichkeitsrechten (Kapitel 2)

💣 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 14)

💣 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 davon aus, dass dies nicht so stimmt. In den folgenden Ausführungen wird angenommen, dass es allein um die Datenerhebung durch Dritte geht. (Seite 50)

💣 Sämtliche Aspekte der „Datenkopie“ sind unter Experten umstritten und werden von Gerichten auf verschiedene Weise angewendet.
- Was bezweckt das Recht auf Datenkopie?
- Bedeutet jeder Wunsch nach Auskunft automatisch auch eine Kopie?
- Wie umfangreich/ausführlich muss die Kopie sein?

Die Rechtsunsicherheit ist enorm. (Seite 58)

💣 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 86)

💣 Was ist eine „Bereitstellung“ von Daten, die zum Recht auf Datenübertragbarkeit führt? Sind nur jene Daten relevant, welche die betroffene Person durch bewusstes Handeln liefert? Unstrittig betroffen sind jene Daten, die eigenhändig per Tastatur eingetippt wurden. Was aber ist mit Logfiles, die versteckt im Hintergrund erzeugt werden? Was ist mit den Videodaten, die entstehen, wenn sich eine Person im Sichtfeld einer Videokamera befindet? Was ist mit den Geo-Daten einer Fitness-Uhr, die an den Anbieter übertragen werden? (Seite 88)

[Ab hier eine Lücke aufgrund der Leseprobe...]

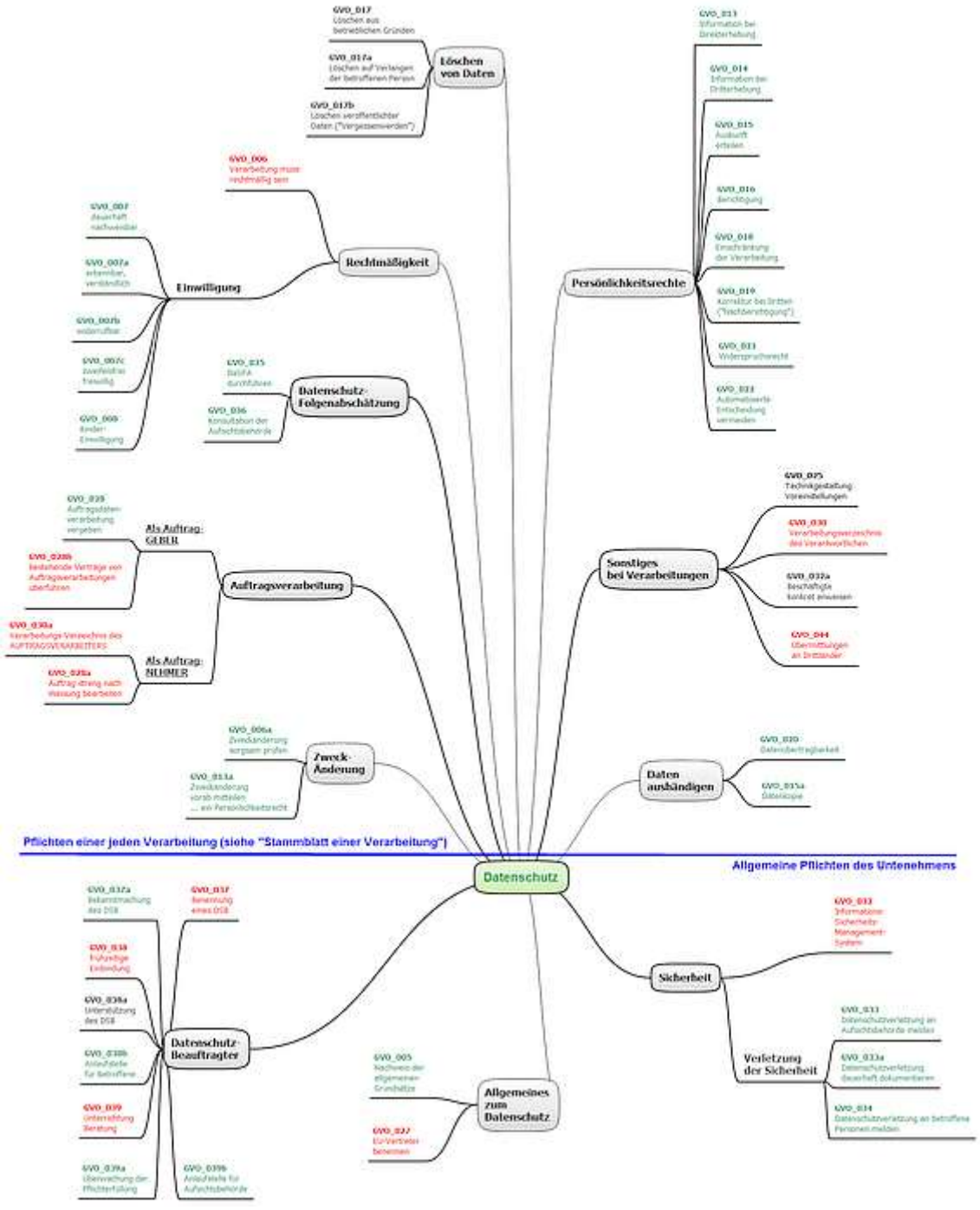
14.5 Mindmap der Pflichten

Anhang

Das folgende Mindmap zeigt die Pflichten im Sinne des Kapitels „Ausrichtung nach Pflichten (Schritt 3)“ auf Seite 13.

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

Das Mindmap finden Sie in voller Qualität in der Datei **PrivazyPlan.zip** (siehe Seite 29) im Unterverzeichnis „_Allgemeines“.



Quelle: PrivazyPlanMindmap_demo.png

14.6 Geführte Tour durch den PrivazyPlan®

Anhang

Vielen Lesern des PrivazyPlan® erscheint das PDF-Dokument zu lang und wirkt daher wenig einladend.

Wir möchten daher allen Lesern eine **geführte Tour** anbieten, um die wichtigsten Kapitel zu durchlaufen. Sie erkennen die Stationen an diesem Bild:

Und hier sind die Stationen:

❶ Navigation im PrivazyPlan®

Wie findet man sich im PrivazyPlan® zurecht? Wie navigiert man hin und zurück? HIER wird das ausführlich erklärt. Inklusive Video.
Lassen Sie sich von dem Seitenumfang des PrivazyPlan® bitte nicht einschüchtern! Stellen Sie sich vor, der PrivazyPlan® ist so eine Art Website im Internet.

❷ Was für Pflichten gibt es im Datenschutz?

In den Bestimmungen der DS-GVO und dem BDSG (und in anderen Gesetzen) verbergen sich eine Menge Pflichten, deren Verstoß bußgeldbewährt ist. Dies ist der Dreh- und Angelpunkt des PrivazyPlan®. Im Kapitel 1.4.3 wird dies näher erläutert.
HIER finden Sie eine kürzest-mögliche Liste dieser Pflichten. Diese sollten Sie unbedingt lesen.

❸ Wo speichert man die eigenen Arbeits-Ergebnisse? Wo finden sich die ausfüllbaren Text-Vorlagen?

Hier im PrivazyPlan® liefert das Kapitel 12 zwar viele Formulare und Checklisten. Doch das reicht nicht aus. Es bedarf ausfüllbarer MS-Word-Dokumente und einem Ort, wo man sie speichern kann. Für all diese Fragen haben wir HIER eine Antwort. Inklusive Video.

❹ IT-Sicherheit systematisch betreiben und dokumentieren mittels ISA+

Im Kapitel 5.1 des PrivazyPlan® wird die IT-Sicherheit ausführlich thematisiert. Im Kapitel 13.4 werden verschiedene Informations-Sicherheits-Managementsysteme (ISMS) vorgestellt. Doch viele Unternehmen können die geforderten Nachweise noch nicht erbringen. HIER weisen wir ganz explizit auf ISA+ hin, welches mit minimalen Mitteln einen ganz respektablen Ansatz liefert. Weniger Aufwand geht nicht.

Warum ist das wichtig? Weil der Nachweis von angemessenen IT-Sicherheitsmaßnahmen der entscheidende Punkt sein kann, wenn es um die Verminderung von Bußgeldern geht. Es geht also um bares Geld.

❺ Transparenz schaffen

Die DS-GVO sichert den betroffenen Personen umfassende Informationsrechte zu. Das ist eine anspruchsvolle Aufgabe für das Unternehmen. HIER werden die sogenannten „Transparenztexte“ erklärt, die jedes Unternehmen vorbereiten und ggf. veröffentlichen sollte.

Warum ist das wichtig? Weil es hier um eine öffentlichkeitswirksame Pflicht geht, die von jeder betroffenen Person (und der Aufsichtsbehörde) sehr einfach geprüft werden kann. Mittlerweile werden ja sogar Bußgelder für mangelnde Transparenz verhängt!

… soweit die Stationen der Tour durch die wichtigsten Kapitel des PrivazyPlan®. In Zukunft werden sicherlich neue Stationen hinzukommen.

Zurück zum Vorwort

14.7 Ausgelagerte Inhalte

Der hier vorliegende PrivazyPlan® verfügt über einen Umfang von über 600 Seiten, doch das ist noch nicht alles. Es gibt noch einige ausgelagerte Dokumente, die verhindern sollen, dass sich dieser Praxisleitfaden zu schnell vergrößert. Derzeit haben diese Dokumente einen Umfang von 321 Seiten.

Die Dokumente sind in der Privazyplan.zip gespeichert (diese Verzeichnisstruktur wird ab Seite 29 erklärt).

Pflichten aufgrund Persönlichkeitsrechten

- **Sensibilisierung zur Nachberichtigung**
  Wenn Daten sich ändern und auch bei anderen Unternehmen („Dritten“) geändert werden müssen, so ist das eine organisatorische Herausforderung, weil die Beschäftigten stets daran denken müssen. Wir liefern eine 1-seitige Sensibilisierung. Seite 85

Dokumentation und Nachweise

- **Testat zum Nachweis von Compliance**
  Ihr Unternehmen benötigt einen knackigen Nachweis zum „Einhaltung der Grundsätze“ gemäß Artikel 5? Wir liefern eine 3-seitige Vorlage. Seite 105

- **Extrem ausführlicher Compliance-Nachweis**
  Sie möchten die Einhaltung aller hier im PrivazyPlan® aufgeführten Pflichten dokumentieren? Dann bietet wir Ihnen ein 28-seitiges Dokument, welches dies vollumfänglich ermöglicht. Seite 105

- **Artikel-5 Nachweis Checkliste**
  Für einen Nachweis der Einhaltung der Grundsätze kann man sich buchstabengenau an die Fragestellungen des Artikel 5 halten. Hierfür liefern wir auf 4 Seiten konkrete Anregungen, die ehemals im Kapitel 3.1.3 enthalten waren. Seite 105

- **Datenschutz-Quickcheck gemäß VdS-10010**
  Der VdS liefert einen Quickcheck mit immerhin 26 Fragen. ~~Wir haben auf 13 Seiten zumindest die Überschriften von der Website zusammenkopiert und stellen Ihnen auf Anfrage gerne auch das vollständige 22-seitige Dokument zur Verfügung.~~

Sicherheit und Datenschutzverletzungen

- **Schutz vor Makroviren (EMOTET)**
  Wie schützt man das Unternehmen vor Makroviren. Wir liefern eine 23-seitige Anleitung mit zahlreichen Bildern. Seite 160

- **Privatsphäre auf PC und Smartphone**
  Wie kann man auf den eigenen Geräten für mehr Privatsphäre sorgen? Wir liefern eine anschauliche 14-seitige Anleitung. Seite 161

- **Mini-ISMS**
  Eine Ultrakurz-Vorlage für ein Informations-Sicherheits-Managementsystem für Kleinstunternehmen. Auf 5 Seiten liefern wir die wesentlichsten Fragestellungen. Seite 425

- **ISA+-Fragebogen (beispielhaft ausgefüllt)**
  Dieser Fragebogen ist eine Möglichkeit um ein minimales Informations-Sicherheits-Managementsystem (ISMS) zu gewährleisten. Auf 28-Seiten Umfang wurden seitens SecureDataService beispielhafte Ausfüllungen vorgenommen. Seite 525

- **Installation von MTA-STS**
  Ein E-Mail-Server sollte dieses Protokoll beherrschen, um ausgehende E-Mails zuverlässig per TLS zu verschlüsseln. Seite 560

Sonstige Pflichten

- **Direktwerbung rechtskonform gestalten**
  Die Werbung per Post, Telefon und E-Mail etc. darf keinen belästigenden Charakter haben. Hierfür steht eine 4-seitige Checkliste zur Verfügung. Seite 273

Formulare

- **Gerüst einer Datenschutzerklärung**
  Warum benötigt eine Website eine Datenschutzerklärung? Was muss sie beinhalten? Wir liefern dazu eine 5-seitige Anleitung. Seite 322

- **Website-Checkliste**
  Es gibt enorm viele datenschutzrelevante Aspekte bei der Gestaltung einer Website. Angefangen beim Hosting, bis hin zu Besucherstatistiken bietet sich ein weites Feld, welches wir auf in einer 22-seitigen Checkliste abarbeiten. Seite 322

- **Aspekte zum HomeOffice**
  Was gilt es im HomeOffice zu beachten? Wir

liefern Anregungen auf 4 Seiten. Seite 324

- **Sensibilisierung zur Transparenz**
  Die Beschäftigten werden auf einer Seite über die Transparenztexte hingewiesen, um letztlich dann auch auf entsprechende Verlangen von Kunden und anderen Mitarbeitern reagieren zu können. Seite 324

- **Checkliste für Videoüberwachung**
  Wie dokumentiert man eine bestehende Videoüberwachung? Welche neuralgischen Punkte gibt es dort? Wir liefern eine 4-seitige Checkliste. Seite 325

- **Sensibilisierung zur Videoüberwachung**
  Wenn Beschäftigte eine neue Videoüberwachung in Erwägung ziehen, dann sollten Sie frühestmöglich die typischen Stolpersteine berücksichtigen. Wir liefern eine 1-seitige Sensibilisierung. Seite 325

- **Theorie zur Interessenabwägung**
  Was ist eine Interessenabwägung und wir kann sie durchgeführt werden? Die Theorie hierzu wird sehr detailliert erklärt. Außerdem liefern wir hier einen konkreten und objektiven Ansatz auf 9 Seiten. Seite 338

- **Gemeinsame Verantwortlichkeit**
  Der Vertrag zur „gemeinsamen Verantwortlichkeit“ gemäß Artikel 26 ist eine knifflige Angelegenheit. Wir liefern eine Vorlage in 3-seitiger Kurzversion und 20-seitiger Langversion. Seite 376

- **Analyse von Geschäftsprozessen**
  Um die Verarbeitungen personenbezogener Daten identifizieren zu können schlägt die VdS-Richtlinie 10010 eine Modellierung anhand der Geschäftsprozesse vor. Dies ist ein sehr guter Ansatz, den wir auf 12 Seiten konkret mit Beispielen aufzeigen. Zu finden in den Formularen zum Verarbeitungsverzeichnis gemäß der Pflicht **[GVO_030]** auf Seite 409

- **On- und Offboarding von Beschäftigten**
  Wenn Mitarbeiter kommen und gehen, so gibt es viele datenschutzrelevante Aspekte zu bedenken. Wir liefern ein 4-seitiges Formular. Seite 427

- **Sensibilisierung zum Whistleblowing**
  Verfügt Ihr Unternehmen über ein Whistleblow-System? Dann sollten Sie die Beschäftigten entsprechend sensibilisieren (und zum Mitmachen auffordern). Wir liefern eine 1 Seite zu diesem Thema. Seite 431

- **Risikopotential-Analysen (speziell)**
  Speziell für Versicherungsmakler haben wir eine Risikopotential-Analyse (RPA) entworfen. Außerdem auch eine RPA übergreifend für alle Verarbeitungen (was am Anfang ziemlich viel Zeit sparen kann). Insgesamt 8 Seiten. Seite 455

Fachinformationen

- **Onlinemeeting mit ZOOM**
  Welche Überlegungen muss man anstellen und welche Dokumente muss man erarbeiten, um ZOOM einsetzen zu können? Wir liefern eine Anleitung und viele Beispieldokumente auf insgesamt 40 Seiten. Seite 647

- **Digitalisierungs-Produkte**
  Wie lässt sich das eigene Geschäftsmodell bzw. das Marketing digitalisieren? In diesem 26-seitigen Dokument liefern wir konkrete Vorschläge und Tipps. Seite 651

- **Leitfaden zum Einstieg in die Cloud**
  Die umfangreiche Auslagerung der Datenverarbeitung an einen Cloud-Service-Anbieter bedarf gründlicher Überlegungen. Auf 11 Seiten liefern wir dazu einen Leitfaden. Seite 658

14.8 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.

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z