Broschüre für die sonstigen Leistungserbringer im Gesundheitswesen

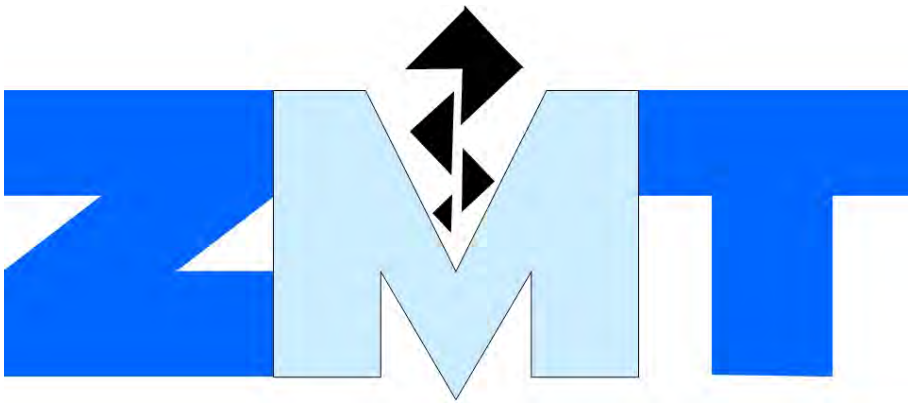
Die neue EU-Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz

erstellt durch

Kramer & Partner
Dipl.-Ing. (FH) Sylvia Kramer und Joachim Kramer GbR
Büro für Datenschutz und Datensicherheit

in Kooperation mit der

ZMT e.V.
Zentralvereinigung medizin-technischer Fachhändler,
Hersteller, Dienstleister und Berater



Inhaltsverzeichnis:

Vorwort:

Bereits seit 1995 beschäftigte sich die europäische Union (EU) mit einheitlichen Datenschutzrichtlinien in der EU. An der damals erlassenen EU-Richtline 95/47/EG haben sich die verschiedenen EU-Staaten mehr oder weniger eng orientiert. So wuchsen die Datenschutzstrukturen in den EU-Staaten sehr unterschiedlich. Deutschland orientierte sich immer sehr eng an den Richtlinien während andere Länder, wie z. B. Irland, das Thema eher vernachlässigten. Dies führte letztendlich dazu, dass viele große US-amerikanische IT-Unternehmen, auch aufgrund lockerer Steuergesetze und der nicht vorhandenen Sprachbarriere, ihren europäischen Sitz nach Irland verlegten. So waren u. a. Microsoft, Google, Facebook, Dell etc. mit ihren europäischen Vertretungen in Irland zu finden.

Das erste Datenschutzgesetz der Welt brachte 1970 Hessen auf den Weg. Im Jahre 1977 zog der Bund nach und verabschiedete die erste Fassung des Bundesdatenschutzgesetzes (BDSG). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts 1983 wurde deutlich, dass die bisherigen Datenschutzgesetze den verfassungsrechtlichen Anforderungen nicht genügten. So fand 1990 die erste große Novellierung des BDSG statt. Diese Fassung ist mit weiteren Novellierungen u. a. im Jahr 2009 noch bis zum 24. Mai 2018 gültig.

Um das Datenschutzniveau und die Gesetzgebung innerhalb der EU zu vereinheitlichen, und auch den Datenaustausch von personenbezogenen Daten zwischen den EU Staaten zu vereinfachen, musste die EU endlich handeln. Dies tat sie jüngst mit der Einführung der Verordnung EU 2016/679, der sogenannten EU-Datenschutzgrundverordnung (DSGVO). Warum die EU ausgerechnet jetzt die Richtlinie durch eine Gesetzgebung ersetzt hat liegt auf der Hand. Einer der Gründe war ein Urteil des Europäischen Gerichtshofs zum Safe Harbor Abkommen. Im so genannten Schrems-Urteil (C-362/14) vom 6. Oktober 2015 wurde das Safe Harbor Abkommen aufgehoben. Bei diesem Projekt ging es grob darum, dass sich US-amerikanische Unternehmen in diesem aufnehmen lassen konnten, indem sie behaupteten, sich den EU Datenschutzrichtlinien anzupassen. Somit war ein Austausch von personenbezogenen Daten mit diesen Unternehmen möglich. Die Kontrolle der Einhaltung der Richtlinien war aber eher als unzureichend zu bezeichnen. Dies ging soweit gut, bis ein österreichischer Facebook Nutzer mit Namen Schrems gegen den Datenschutz bei Facebook klagte. Dieser Rechtsstreit endete vor dem EuGH und Herr Schrems bekam recht. Im Anschluss daran wurde das Safe Harbor Abkommen aufgelöst. Dieses Urteil, die Bespitzelungsaktionen der Amerikaner in Europa und auch die Notwendigkeit eines Datenaustausches im Rahmen von Terrorbekämpfung und Zuwanderung in der EU brachte schließlich die im Mai 2016 verabschiedete DSGVO auf den Weg. Diese tritt mit einer zweijährigen Übergangsfrist am 25. Mai 2018 in Kraft.

Da die DSGVO auch über der nationalen Gesetzgebung schwebt, müssen in Deutschland die Gesetze entsprechend der DSGVO angepasst werden. Das BDSG (neu) wurde als Teil des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) beschlossen. Diese neueste Fassung des BDSG wird am 25. Mai 2018 zusammen mit der Datenschutzgrundverordnung (DSGVO) in Kraft treten und das noch aktuelle Bundesdatenschutzgesetz (BDSG) vollständig ersetzen.

Andere Gesetze, die auch Paragraphen beinhalten die den Datenschutz betreffen, behalten ihre Gültigkeit, insofern sie mit der DSGVO in Einklang stehen oder müssen angepasst werden (z. B.: SGB, StGB, kirchliche Datenschutzgesetze, Krankenhausgesetze, Rettungsdienstgesetze, Berufsordnungen etc.). Auch die 16 Landesdatenschutzgesetze müssen den Forderungen der DSGVO entsprechen und angepasst werden.

Die DSGVO enthält 99 Artikel mit 173 Erwägungsgründen sowie fast 70 Öffnungsklauseln in nationale Gesetzgebungen. Zur Zeit herrscht immer noch eine gewisse Unsicherheit, wie einzelne Forderungen aus der DSGVO praktikabel und gesetzeskonform umgesetzt werden sollen. Es gibt durch die großen Verbände erst wenig Muster und auch die Aufsichtsbehörden der einzelnen Bundesländer halten sich noch bedeckt.

Diese Broschüre soll Ihnen einen Überblick geben, was sich durch das Inkrafttreten der DSGVO und des BDSG (neu) ändern wird und was zu erledigen bzw. umzusetzen ist. Diese Broschüre erhebt nicht den Anspruch auf Vollständigkeit. So wurde auf die Forderungen privacy by design und privacy by default nicht näher eingegangen. Sie kann nur einen kleinen Überblick bieten und auch nur Empfehlungen aussprechen, die auf unserer Erfahrung und Einschätzung beruhen. Es empfiehlt sich zusätzlich immer den Gesetzestext (Artikel und Erwägungsgründe) zu lesen sowie einen Kommentar zu den jeweiligen Bestimmungen.

Der Datenschutz ist Ländersache:

In Deutschland ist der Datenschutz Ländersache, d. h. jedes Bundesland hat eine eigene Aufsichtsbehörde und einen bzw. eine Landesdatenschutzbeauftragte(n). Die einzelnen Landesdatenschutzbeauftragten haben keine direkten Vorgesetzten mehr, treffen sich aber mehrmals im so genannten Düsseldorfer Kreis. Dieser ist ein Zusammenschluss der deutschen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Ziel des Gremiums ist es, einen Konsens bei der Auslegung, Anwendung und Weiterentwicklung des Datenschutzrechts zu finden.

Für nichtöffentliche Stellen gelten grundsätzlich das Bundesdatenschutzgesetz (BDSG neu) und die Datenschutzgrundverordnung (DSGVO) ab 25.05.2018. Beide Gesetze enthalten aber auch Paragraphen bzw. Artikel für den öffentlichen Bereich. Die Landes-datenschutzgesetze gelten nur für die öffentlichen Stellen des jeweiligen Bundeslandes.

Ferner gibt es noch eine Bundesdatenschutzbeauftragte (BfDI). Diese ist den Landes-datenschutzbeauftragten nicht vorgesetzt und kümmert sich um den Datenschutz bei den übergeordneten staatlichen Stellen (Post, Bahn, Bundeswehr, Bundesnachrichtendienst etc.).

Ferner gilt das so genannte Marktortprinzip (Art. 3 Abs. 2 DSGVO). Dies bedeutet, dass immer die Aufsichtsbehörde zuständig ist, wo die Daten der Betroffenen aus der EU verarbeitet werden. Beispiel: Die Firma Amazon hat ihren Sitz in den USA. Somit unterläge sie nicht dem europäischen Datenschutzrecht. Sie unterhält aber ein Auslieferungs- und Logistikzentrum in Koblenz. Die Daten der von dort aus belieferten Personen sowie die Mitarbeiterdaten der in Koblenz tätigen Mitarbeiter unterliegen der DSGVO und dem BDSG (neu). Die Zuständige Aufsichtsbehörde wäre „Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz“.

Hat ein Unternehmen in Deutschland eine Hauptstelle und mehrere nicht selbständige Niederlassungen in verschiedenen Bundesländern, ist für den Datenschutz immer die Aufsichtsbehörde, die im gleichen Bundesland wie die Hauptstelle ihren Sitz hat, zuständig.

Merke:
Der Datenschutz ist Ländersache.
Es gilt das Marktortprinzip.

Der Datenschutzbeauftragte:

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten (DSB) wenn die Kerntätigkeit in der Verarbeitung von besonderen Arten personenbezogener Daten (Gesundheitsdaten) liegt (Art. 37 Abs. 1C DSGVO).

Der Verantwortliche und der Auftragsverarbeiter benennen einen DSB wenn in der Regel mehr als 10 Beschäftige mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind (§ 38 Abs. 1 BDSG (neu)). Dies gilt für alle Betriebe die personenbezogene Daten verarbeiten.

Nimmt der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutzfolgeabschätzung unterliegen, haben sie unabhängig von der Anzahl der Beschäftigten einen DSB zu bestellen § 38 BDSG (neu). Eine Datenschutzfolgeabschätzung muss auf jeden Fall vorgenommen werden wenn sensiblen Daten wie Gesundheitsdaten, Sexualdaten, Daten über strafrechtliche Verurteilungen, Videoüberwachung, Profiling etc. verarbeitet werden.

Die Kontaktdaten müssen veröffentlicht werden (z. B. auf der Website) und der für den Verantwortlichen zuständigen Aufsichtsbehörde mitgeteilt werden (Art. 37 Abs. 7 DSGVO). Dafür reicht ein formloses Schreiben an die Behörde. Zur Zeit sind die Aufsichtsbehörden damit beschäftigt, eine Bundesland übergreifende Online-Plattform aufzusetzen, damit die Unternehmen ihren Datenschutzbeauftragten elektronisch melden können.

Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DSGVO aufgelistet. Er unterrichtet und berät den Verantwortlichen und die Beschäftigten hinsichtlich ihrer Pflichten aus der DSGVO und die anderen, für das Unternehmen relevanten, Gesetze die den Datenschutz betreffen. Er überwacht die Einhaltung der Datenschutzgesetze und sensibilisiert bzw. schult Mitarbeiter, die mit der Verarbeitung von personenbezogenen Daten betraut sind. Er berät auf Anfrage bei der Datenschutzfolgeabschätzung und überwacht die Durchführung. Er ist Anlaufstelle für die Aufsichtsbehörde und Mitarbeiter.

Die Stellung des Datenschutzbeauftragten ist im Art. 38 DSGVO hinreichend erläutert. Er bei seiner Tätigkeit weisungsfrei und zur besonderen Verschwiegenheit nach § 203 Abs. 2a StGB verpflichtet.

Merke:
Für Leistungserbringer im Gesundheitswesen ist die Bestellung eines Datenschutzbeauftragten verpflichtend. Als Datenschutzbeauftragter kann eine interne Person bestellt werden oder der Datenschutzbeauftragte ist Externer und arbeitet auf Grundlage eines Dienstleistungsvertrags. In beiden Fällen muss der DSB ausreichend qualifiziert sein und schriftlich bestellt werden. Die Kontaktdaten müssen veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

Auflistung der Aufsichtsbehörden:

Baden-Württemberg
Der Landesbeauftragte
für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Postfach 10 29 32
70025 Stuttgart

Bayern
Landesamt für Datenschutzaufsicht
Postfach 606
91511 Ansbach

Berlin
Berliner Beauftragter
für Datenschutz und Informationsfreiheit
Friedrichstr. 219
10969 Berlin

Brandenburg
Die Landesbeauftragte
für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Bremen
Der Landesbeauftragte
für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen
Postfach 10 03 80
27503 Bremerhaven

Hamburg
Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C)
20095 Hamburg

Hessen
Der Hessische Datenschutzbeauftragte
Postfach 31 63
65021 Wiesbaden

Mecklenburg-Vorpommern
Der Landesbeauftragte
für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Lennéstraße 1 , Schloss Schwerin
19053 Schwerin

Niedersachsen
Die Landesbeauftragte
für den Datenschutz Niedersachsen
Postfach 221
30002 Hannover

Nordrhein-Westfalen
Der Landesbeauftragte
für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf

Rheinland-Pfalz
Der Landesbeauftragte
für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Postfach 30 40
55020 Mainz

Saarland
Unabhängiges Datenschutzzentrum Saarland
Landesbeauftragte für Datenschutz und Informationsfreiheit
Postfach 10 26 31
66026 Saarbrücken

Sachsen
Der Sächsische Datenschutzbeauftragte
Postfach 12 09 05
01008 Dresden

Sachsen-Anhalt
Landesbeauftragter für den Datenschutz Sachsen Anhalt
Postfach 19 47
39009 Magdeburg

Schleswig-Holstein
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Postfach 71 16
24171 Kiel

Thüringen
Der Thüringer Landesbeauftragte für den Datenschutz
Postfach 90 04 55
99107 Erfurt

Die verschiedenen Datenkategorien:

Anonyme Daten, anonymisierte Daten und Statistikdaten finden keinerlei Anwendung im BDSG (neu) bzw. in der DSGVO. Dies gilt immer, wenn ein Rückschluss auf eine natürliche Person ausgeschlossen werden kann. Z. B.: in Köln fahren 75.000 Menschen einen Mercedes und 150.000 einen VW etc.

Pseudonymisierte Daten lassen einen Rückschluss auf eine Person zu und werden wie personenbezogene Daten behandelt, können aber unter bestimmten Umständen wie anonymisierte Daten verarbeitet werden. Hat man von einer Person nur ihre Personalausweisnummer (ohne ihren Namen) weiß man normalerweise nicht wer hinter dieser Nummer steckt. Der Staat weiß aber welche Person sich hinter dieser Personalausweisnummer verbirgt (Art. 4 Nr. 5 DSGVO).
Beispiel: Gibt man Daten zur Fertigung eines Hilfsmittels an einen Hersteller weiter und benutzt dafür nur die eigene Kundennummer als Kommissionsnummer, werden an diesen Hersteller keine personenbezogenen Daten weitergegeben. Dies wird anhand eines Beispiels für die Fertigung von Einlagen über einen Hersteller bzw. Dienstleiter deutlicher:

Weitergabe an einen Hersteller:
Max Mustermann, geb. 22.07.1964, Gewicht 92kg, Maßblatt / Trittspur
(Weitergabe personenbezogener Gesundheitsdaten an einen Dritten)

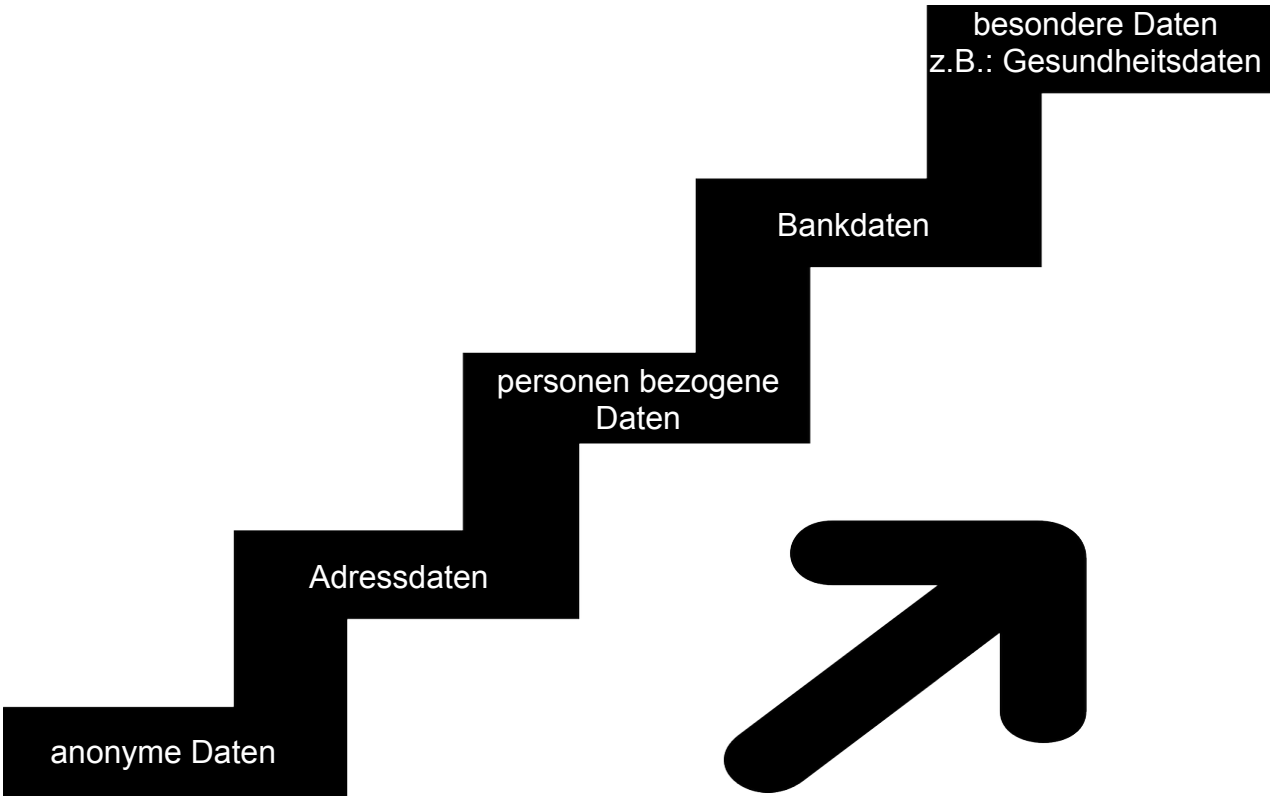
Kunde: 4711, Gewicht 92kg, Maßblatt / Trittspur
(keine Weitergabe personenbezogener Daten – der Hersteller hat keine Möglichkeit herauszufinden wer sich hinter 4711 verbirgt.)

Personenbezogene Daten sind Informationen über eine identifizierte oder identifizierbare natürliche Person „betroffene Person“ die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen, sozialen Identität beinhalten. Im alten BDSG sprach man von sachlichen oder persönlichen Verhältnissen einer bestimmten oder bestimmbaren Person (Art. 4 Nr. 1 DSGVO).

Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person „betroffene Person“, die von einer in § 35 SGB I des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden (§ 67 SGB X Abs. 1).

Besondere Kategorien von Daten sind unter anderem „genetische Daten“, „biometrische Daten“ und „Gesundheitsdaten“ (Art. 4 Nr. 13,14,15). Diese Daten unterliegen strengeren Auflagen bei der Verarbeitung. Werden solche Daten in irgendeiner Weise verarbeitet oder übermittelt, ist in jedem Fall eine Datenschutzfolgeabschätzung vorzunehmen.

Sensibilität der Daten:



Merke:
Je sensibler die Daten sind, bzw. je mehr Gefahren für die Rechte und schutzwürdigen Interessen der Betroffenen drohen, desto höher müssen die technischen und organisatorischen Maßnahmen im Datenschutz sein.

Werden Gesundheitsdaten verarbeitet, weitergegeben bzw. übermittelt ist auf jeden Fall eine Datenschutzfolgeabschätzung durchzuführen.

Verarbeitung von Daten:

Erhebung von Daten ist: Die Auf- oder Entgegennahme von Daten zum Zweck der Erfassung oder Verarbeitung.

Verarbeitung von Daten ist: das Erfassen, Speichern, Bearbeiten, Löschen, Sperren, Drucken, Aufbereiten oder Zusammenführen von Daten.

Nutzung von Daten ist: die Verwendung der Daten für einen bestimmten Zweck.

Übermittlung von Daten ist: die Übertragung von Daten zu einer internen oder externen Stelle für einen bestimmten Zweck.

Merke:
Die DSGVO definiert in Art. 4 Nr. 2 die Verarbeitung. Diese beinhaltet alle oben angeführten Punkte die früher, im alten BDSG, einzeln genannt waren. Um Daten „verarbeiten“ zu können, wird immer eine Rechtsgrundlage benötigt.

Rechtsgrundlagen für die Verarbeitung von Daten:

Es besteht eine gesetzliche Regelung:
Die Verarbeitung (Übermittlung) ist in einem Gesetz geregelt (z. B.: AO, SGB, DEÜV, DSGVO, BDSG (neu) etc.). Ist die Verarbeitung oder die Übermittlung von Daten für den konkreten Zweck in einem Gesetz geregelt, braucht von der betroffenen Person keine Einwilligungserklärung für diesen konkreten Zweck eingeholt werden.

Beispiel: im Rahmen der Lohnabrechnung müssen Daten an Finanzämter, Krankenkassen, Berufsgenossenschaften etc. gemeldet werden. Dies kann ohne Einwilligung des Arbeitnehmers erfolgen.

Die Einwilligung des Betroffenen:
Der Betroffene willigt schriftlich ein. Wichtig ist, dass die Einwilligung transparent ist (Zweck, Empfänger, welche Daten etc.), die Einwilligung in einer einfachen Sprache verfasst ist, freiwillig erfolgt und auch ein Widerrufsrecht beinhaltet.

Beispiel: Das Unternehmen beabsichtigt Fotos der Mitarbeiter auf der firmeneigenen Webseite einzustellen. Neben dem Bild soll auch der Name des Mitarbeiters sowie seine Tätigkeit im Betrieb erwähnt werden. Hierfür ist eine Einwilligungserklärung des Mitarbeiters notwendig.

Auftragsverarbeitung:
Wird ein „Dritter“ bzw. ein „Dienstleister“ in die Verarbeitung involviert, kann dies mit Hilfe einer Vereinbarung zur Auftragsverarbeitung (Vertrag) gem. Art. 28 bzw. Art. 29 DSGVO erfolgen. Wichtig ist, dass der Dienstleister (Auftragsverarbeiter) sorgfältig ausgewählt wird und ausreichend Garantien für die datenschutzkonforme Durchführung der Verarbeitung übernimmt. Der Auftragsverarbeiter darf die Daten nur nach den Weisungen des Verantwortlichen (Auftraggeber) und für den im Vertrag genannten Zweck verarbeiten. Der Auftragsverarbeiter ist dem Betroffenen nach Art. 13 DSGVO mitzuteilen.

!!! Trotz Auftragsverarbeitung kann bei Berufsgeheimnisträgern eine Entbindung von der Schweigepflicht nach § 203 StGB nötig sein. Auch bei einer Einwilligung muss diese bei Berufsgeheimnisträgern um die Schweigepflichtentbindung erweitert werden.

Merke:
Ohne Rechtsgrundlage geht gar nichts. Die Grundsätze für die Verarbeitung personenbezogener Daten sowie die Rechtmäßigkeit der Verarbeitung sind in Art. 6 und Art. 7 der DSGVO aufgeführt. Ferner werden die rechtlichen Grundlagen in den §§ 22–31 im BDSG (neu) definiert.

Die neuen Transparenzgebote:

Es gibt neue Transparenzgebote nach Art. 13 DSGVO und § 32 BDSG (neu) wenn Daten direkt beim Betroffenen erhoben werden. Neuerdings muss eine betroffene Person (Kunde, Patient, Mandant, Klient) bei der Erhebung ihrer Daten über einige Punkte aufgeklärt werden.

Diese Aufgabe hat auch ein Auftragsverarbeiter, wenn dieser nicht sicher sein kann, dass der Betroffene bereits unterrichtet wurde, dass er in die Verarbeitung involviert ist (Art. 14 DSGVO bzw. § 33 BDSG (neu)). Beruft ein Auftragsverarbeiter sich aber auf den letzten Punkt des Art. 13 DSGVO braucht er dieser Transparenzpflicht nicht erneut nachkommen, wenn er sicher ist, dass der Verantwortliche bereits den Betroffenen informiert hat.

Im Rahmen der Nachweispflicht muss der Betroffene bestätigen, dass er aufgeklärt wurde (im Internet evtl. durch einen bestätigenden Klick – sonst evtl. durch Unterschrift auf einem Formular).

Über folgende Punkte muss die betroffene Person zum Zeitpunkt der Datenerhebung aufgeklärt werden:

- Name und Kontaktdaten des Verantwortlichen
- ggf. Name des Datenschutzbeauftragten
- Zweck und Rechtsgrundlage für die Verarbeitung der Daten
- welche Interessen vom Verantwortlichen oder einem Dritten verfolgt werden
- Empfänger oder Kategorien von Empfängern von personenbezogenen Daten
- die Dauer der Speicherung bzw. die Kriterien für die Festlegung der Dauer
- Hinweis auf die Rechte des Betroffenen (Auskunft, Löschung etc.)
- das Widerrufsrecht einer evtl. erteilten Einwilligung
- das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
- ob die Bereitstellung ihrer Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und ob die Bereitstellung der Daten Pflicht ist und welche Folgen eine Nichtbereitstellung hätte
- das Bestehen einer automatisierten Einzelentscheidung inkl. Profiling und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und Auswirkungen einer derartigen Verarbeitung der betroffenen Person
- werden die Daten für andere Zwecke weiter verarbeitet so informiert der Verantwortliche den Betroffenen über den Zweck (siehe oben)

Dies braucht nicht zu geschehen, wenn der Betroffene bereits über alle Informationen verfügt.

Merke:
Die neuen Transparenzpflichten müssen umgesetzt werden. Wie sie praktikabel umzusetzen sind, bleibt bisher unklar. Ob ein „Aushang“ reicht oder ob die betroffene Person die Aufklärung durch Unterschrift bestätigen muss ist ebenfalls nicht klar. Bei einer Datenerhebung auf einer Website kann man die Transparenzgebote leicht einbinden.

Die Rechte der Betroffenen:

- Recht auf Auskunft (Art. 15 DSGVO und § 34 BDSG (neu))
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO und § 35 BDSG (neu))
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO - eine Berechnung ist evtl. zulässig)
- Widerspruchsrecht (Art. 21 DSGVO und § 36 BDSG (neu))

Ein Großteil der Rechte der betroffenen Person gab es bisher im alten BDSG auch. Neu hinzu gekommen sind das „Recht auf Vergessenwerden“ und das Recht auf Datenübertragbarkeit.

Beim „Recht auf Auskunft“ hat die betroffene Person das Recht zu erfahren, welche Daten für welchen Zweck verarbeitet wurden, die Empfänger der Daten, wie lange die Daten gespeichert werden bzw. welche Kriterien es für die Speicherdauer gibt. Ferner muss die betroffene Person auf Bestehen eines Rechts auf Löschung bzw. auf Einschränkung der Verarbeitung und das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde informiert werden. Wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden, muss über die Herkunft der Daten und Angaben, ob Scoring oder Profiling Verfahren eingesetzt wurden inklusive der dort involvierten Logik, sowie die Auswirkungen der Entscheidung (Art. 15 Abs. 1 DSGVO) unterrichtet werden. Der Verantwortliche muss eine Kopie der Daten, die Gegenstand der Verarbeitung sind, anfertigen. Auf Antrag hat die betroffene Person auch das Recht, die Daten in einem elektronischen Format zu erhalten (Art. 15 Abs. 3 DSGVO). Verlangt die betroffene Person mehrere Kopien, ist eine Berechnung der Verwaltungskosten zulässig.

Die betroffene Person hat das „Recht auf Berichtigung“ ihrer Daten beim Verantwortlichen. Dieser hat die Berichtigung bzw. Vervollständigung der Daten unverzüglich vorzunehmen (Art.16 DSGVO).

Werden Daten zu Unrecht gespeichert oder unterliegen sie keinerlei Zweckbindung und es gibt keine gesetzlichen Aufbewahrungsfristen, kann die betroffene Person von ihrem „Recht auf Löschung“ Gebrauch machen. Dies gilt auch wenn die betroffene Person eine erteilte Einwilligungserklärung widerruft. Wurden die Daten durch den Verantwortlichen öffentlich (z. B. Internet) gemacht, hat er auch unter Berücksichtigung der ihm zur Verfügung stehenden Mittel dafür Sorge zu tragen, dass auch dort die Daten gelöscht werden. Das „Recht auf Vergessenwerden“ soll dem bekannten Spruch: „Das Internet vergisst nichts.“ entgegenwirken. Wurden Daten weitergegeben teilt der Verantwortliche den Empfängern mit, dass die betroffene Person vom ihrem Recht auf Löschung bzw. Einschränkung der Verarbeitung Gebrauch gemacht hat.

Übt eine betroffene Person das „Recht auf Einschränkung der Verarbeitung“ aus, kann sie anstelle der Löschung verlangen, dass die Daten stattdessen nicht mehr verwendet werden. Dies dient dann z. B. einer Beweissicherung wenn Daten zu Unrecht verarbeitet wurden. Das gleiche Recht gilt auch, wenn eine betroffene Person die Löschung ihrer Daten verlangt, diese aber einer gesetzlichen Aufbewahrungsfrist unterliegen und der Verantwortliche diese nicht löschen darf.
Neu in der DSGVO ist das „Recht auf Datenübertragbarkeit“. Hierbei hat eine betroffene Person das Recht ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen (Unternehmen) zu übermitteln. Ferner kann sie erwirken, dass die Daten direkt von einem Verantwortlichen zum anderen übertragen werden. Z. B.: ist eine betroffene Person schon langjähriger Kunde in der Arztpraxis AB und wechselt den Arzt, kann sie verlangen, dass die Arztpraxis AB ihre Daten zur Arztpraxis XY überträgt. Wie dies in der Praxis umgesetzt werden kann ist noch nicht klar. In vielen Fällen wird es vorkommen, dass Unternehmen mit unterschiedlichen Programmen bzw. Branchenlösungen arbeiten und diese untereinander keine Schnittstelle haben.

Das „Recht auf Widerspruch“ gilt an mehreren Stellen, z. B. kann eine Person eine erteilte Einwilligungserklärung mit der Wirkung für die Zukunft widerrufen. Z. B.: werden auf der Unternehmenswebseite Fotos von Mitarbeitern mit deren Namen abgestellt, erfordert dies die explizite, freiwillige und schriftliche Einwilligung der betroffenen Person. Möchte die Person aus irgendwelchen wichtigen Gründen nicht mehr, dass ihr Bild dort zu sehen ist, kann sie die damals erteilte Einwilligung widerrufen und das Foto ist von der Website zu nehmen. Bei Direktwerbung und bei der Zusendung von Newslettern muss spätestens zum Zeitpunkt der ersten Kontaktaufnahme auf das Widerrufsrecht hingewiesen werden. Dies muss bei jeder Werbung und bei jedem Newsletter immer wieder erwähnt werden.

Merke:
Übt eine betroffene Person ihre Rechte aus, hat der Verantwortliche dem Folge zu leisten. Es ist darauf zu achten, dass alle Vorgänge dokumentiert werden. Die Rechte des Betroffenen ersetzen nicht die Transparenzgebote.

Anforderungen an eine Einwilligungserklärung:

Die Einwilligung in die Verarbeitung ihrer personenbezogenen Daten durch die betroffene Person ist zentraler Bestandteil des Datenschutzrechts. Aufgrund des Grundrechts der informationellen Selbstbestimmung kann jeder Bürger für sich entscheiden (mit Ausnahmen), wer welche Informationen über ihn erhält. Während sich der Art. 6 DSGVO mit der „Rechtmäßigkeit der Verarbeitung“ beschäftigt verweist dieser direkt in Absatz 1a) auf die Einwilligungserklärung.

Der Art. 7 DSGVO befasst sich mit den Bedingungen bzw. Anforderungen an eine Einwilligungserklärung. Beruht die Verarbeitung von Daten der betroffenen Person auf einer Einwilligung, so muss der Verantwortliche nachweisen können, dass diese erteilt wurde, d. h. Einwilligungserklärungen müssen zum Zweck der Nachweisbarkeit archiviert werden. Die Einwilligung muss leicht verständlich formuliert sein und den Sachverhalt klar erläutern. Sie darf grundsätzlich nicht gegen die DSGVO verstoßen und muss freiwillig erteilt werden. Die Einwilligungserklärung muss ein Widerrufsrecht beinhalten. Den Widerruf zu erteilen, muss so einfach sein, wie die Einwilligung abzugeben.

Für Kinder gelten besondere Bedingungen in Bezug auf Dienste der Informationsgesellschaft (Internet). Hier geht der Art. 8 DSGVO davon aus, dass eine Einwilligung ab dem 17. Lebensjahr in Ordnung ist. Ansonsten müssen die Eltern einwilligen.

Die Bedingungen für die Einwilligungen gelten sowohl für schriftlich erteilte Einwilligungen die direkt mit der betroffenen Person vorgenommen werden als auch für Einwilligungserklärungen im Internet z. B. auf einer Website für die Zusendung eines Newsletters.

Das Muster einer einfachen Einwilligungserklärung für das Verwenden von Mitarbeiterfotos für den Zweck der Veröffentlichung finden Sie auf der nächsten Seite.

Merke:
Alte Einwilligungserklärungen sind zu überprüfen, ob diese noch den Bedingungen der DSGVO entsprechen. Neue Einwilligungserklärungen sind entsprechend zu erstellen.

Mustereinwilligungserklärung für die Verwendung von Mitarbeiterfotos:

Firmenname, Straße, Hausnummer, PLZ und Ort (alternativ Firmenstempel)

Einwilligung

gemäß Artikel 6 Abs. 1 a) DSGVO

Mitarbeiter(in)

Name, Vorname: _____

Straße Hausnummer: _____

PLZ, Ort: _____

Geb.-datum: _____

Hiermit erkläre ich mich ausdrücklich und nach vollständiger Aufklärung des Sachverhaltes damit einverstanden und willige freiwillig ein, dass mein Foto in der Abbildung wie vorgelegt und von mir zur Kenntnis genommen, von der Firmenname für folgende Veröffentlichungen verwendet werden darf:

- ☐ Im Internet auf der Homepage unserer Firma (auch mit Name und Tätigkeit)
- ☐ Abbildung in Fachzeitschriften
- ☐ für Schulungszwecke auch dann, wenn nicht bei der Firmenname Beschäftigte an der Schulung teilnehmen
- ☐ Abbildungen meiner Person bei der Erstellung von Collagen, die nicht nur intern ausgestellt werden, sondern auch öffentlich zum Aushang kommen.
- ☐ Abbildungen meiner Person in Fotobüchern und -alben, z. B. bei Ausfahrten, Ausflügen, Urlaub mit Betreuern etc.
- ☐ Weiterhin gilt meine Einwilligungserklärung für:
  (genaue Beschreibung der weiteren Verwendung der Abbildung bzw. des Fotos)

  _____

  _____

Diese Einwilligung kann jederzeit für die Zukunft gegenüber dem Arbeitgeber widerrufen werden. Wenden Sie sich hierzu an die oben genannte Stelle.

_____ _____

Ort, Datum

rechtsverbindliche Unterschrift des Betroffenen bzw. des gesetzl. Vertreters

Verzeichnis von Verarbeitungstätigkeiten:

Mit Einführung der DSGVO muss ein Unternehmen nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies ist nur eine von mehreren, neuen Vorgaben zur Dokumentationspflicht. Bei der Einhaltung aller gesetzlichen Vorgaben wird das Verzeichnis aber eine führende Rolle spielen, denn es enthält eine Dokumentation und Übersicht über alle eingesetzten Verfahren bzw. Prozesse, bei denen personenbezogene Daten verarbeitet werden. Die Forderung ist nicht neu, denn bereits das "alte" BDSG verpflichtete die verantwortliche Stelle zur Führung eines Verfahrensverzeichnisses.

Die Verpflichtung zur Führung dieses Verzeichnisses hat nicht nur der für die Verarbeitung Verantwortliche sondern gegebenenfalls auch ein Auftragsverarbeiter, der die Daten nur im Rahmen einer Auftragsverarbeitung bearbeitet.

Neben dem angesprochenen "Verzeichnis von Verarbeitungstätigkeiten" finden sich in der DSGVO eine Vielzahl von Normen und Regelungen, die einer Dokumentierung der getroffenen Maßnahmen bedürfen. Ferner schafft die DSGVO neue Prozesse, die etabliert, gelebt und wahrgenommen werden müssen. Bei dieser Vielzahl von Anforderungen verliert man schnell den Überblick. Daher bietet sich, gerade für größere Unternehmen mit einer Vielzahl von Prozessen bei denen personenbezogene Daten verarbeitet werden, die Einführung eines Datenschutzmanagementsystems an. Gibt es bereits vorhandene Managementsysteme z. B. für QM, Compliance oder Risikomanagement, kann es Sinn machen das Datenschutzmanagement dort zu integrieren, um Synergien zu nutzen.

Das Aufsichtsbehörde in Niedersachsen (die Landesbeauftragte für den Datenschutz Niedersachsen) hat umfangreiche Hinweise zum Verzeichnis der Verarbeitungstätigkeiten herausgegeben. Diese sind unter dem Link:
https://www.lfd.niedersachsen.de/download/120050
abrufbar und müssen nur noch um die technischen und organisatorischen Maßnahmen im Datenschutz ergänzt werden.

Eine Ausnahme zur Pflicht vom Führen des Verzeichnisses der Verarbeitungstätigkeiten besteht für Unternehmen mit weniger als 250 Beschäftigten, wenn diese keine kritischen Datenverarbeitungen wie Scoreing vornehmen oder keine besonderen Daten wie z. B. Gesundheitsdaten verarbeiten.

Merke:
Die Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten besteht für jeden Betrieb der Gesundheitsdaten verarbeitet, unabhängig von der Anzahl der Beschäftigten. Für jedes Verfahren bzw. Prozess muss dies separat erstellt werden, wobei sich viele Punkte überschneiden bzw. wiederholen.

Mindestinhalt für ein „Verzeichnis von Verarbeitungstätigkeit“:

1) Name und Kontaktdaten
   - des für die Verarbeitung verantwortlichen (natürliche oder juristische Person)
   - eines ggf. mit ihm geimnsamen Verantwortlichen (gem. Art. 26 DSGVO)
   - eines evtl. Verantwortlichen in einem Drittland
   - des Datenschutzbeauftragten

   Hier müssen jeweils die postalische, telefonische und elektronische Erreichbarkeit angegeben und der Name des Verantwortlichen genannt werden.

2) Zweck der Verarbeitungstätigkeit (jeweils einzeln zu betrachten)
   - Datenweitergabe an einen Steuerberater zur Lohnabrechnung
   - Datenweitergabe der Buchhaltung an einen Steuerberater
   - Arbeitszeiterfassung
   - Videoüberwachung
   - Kundendatenpflege mit Hilfe einer Brachenlösung
   - Fernwartung der Branchenlösung
   - Serverhosting
   - Datenweitergabe an einen Hersteller zum Zweck der Hilfsmittelfertigung
   - Abrechnung von Rezepten / Verordnungen / Leistungsnachweisen über ein Rechenzentrum
   - Übertragung elektronischer Kostenvoranschläge an Kostenträger
   - etc.

   Sinnvoll ist hier eine kurze Beschreibung was mit den Daten passiert wie z. B. Übermitteln der Mitarbeiterdaten an den Steuerberater zum Zweck der Lohnabrechnung und Meldung der Daten an gesetzliche Stellen im Rahmen der gesetzlichen Vorgaben.

3) Rechtsgrundlage der Verarbeitung

   Bei der Datenweitergabe von Rezepten / Verordnungen / Leistungsnachweisen an ein Abrechnungszentrum z. B. folgende Rechtsgrundlagen:

   - bei gesetzlich Versicherten: § 302 SGB V
   - bei privat Versicherten: die explizite schriftliche Einwilligungserklärung ggf. mit Entbindung von der Schweigepflicht nach Art. 7 DSGVO und ggf. Entbindung nach § 203 StGB
   - Auftragsverabreitung nach Art. 28 und 29 DSGVO

4) Beschreibung der Kategorien der betroffenen Personen z. B.:
   - Mitarbeiter / Beschäftigte
   - Kunden / Patienten
   - Lieferanten
   - Interessenten
   - Abonnenten
   - etc.

4) Beschreibung von Kategorien personenbezogener Daten (Daten der betroffenen Person):

Bei der Datenweitergabe von Rezepten / Verordnungen / Leistungsnachweisen an ein Abrechnungszentrum z. B. folgende Datenkategorien:

- Versichertendaten
  - Adressdaten
  - Geburtsdatum
  - Angaben zur Krankenversicherung (wie Versichertennummer, Kostenträger etc.)
  - Angaben zum ausstellenden Arzt bzw. Krankenhaus
  - Angaben zur verordneten Leistunge bzw. zum Hilfsmittel
  - Gesundheitsdaten evtl. mit Diagnosen

Die Angaben auf einzelne "Feldebenen" herunterzubrechen macht an dieser Stelle nur wenig Sinn, denn dadurch wird das Verzeichnis zu unflexibel und unübersichtlich. Hier kann man Datenfelder zu sinnvollen Kategorien zusammenfassen (z. B.: Adressdaten sind Name, Straße, Hausnummer, Ort, Bundesland, Staat. Kontaktdaten beinhalten die Adressdaten und zusätzlich Angaben wie Tel.-Nr., Fax-Nr., Mobilfunknummer, E-Mailadresse etc.)

5) Empfänger bzw. Kategorien von Empfängern (auch in Drittländern):

Bei der Datenweitergabe von Rezepten / Verordnungen / Leistungsnachweisen an ein Abrechnungszentrum z. B. folgende Adressangaben:

- Abrechnungszentrum XYZ
- Straße, Hausnummer
- PLZ, Ort

Empfänger können aber auch sinnvollerweise in Kategorien zusammengefasst werden, z. B.: Sozialversicherungsträger, Finanzämter etc. Empfänger können aber auch interne Stellen (innerhalb des Unternehmens) sein, z. B.: Daten aus der Zeiterfassung gehen in die interne Lohnbuchhaltung.

6) Die vorgesehenen Firsten für die Löschung von personenbezogenen Daten bzw. deren gesetzliche Aufbewahrungsfristen

- 10 Jahre für abrechnungsbegründende Unterlagen
- 6 Jahre für Handel- und Geschäftsbriefe
- etc.

7) Eine allgemeine Beschreibung der für den Datenschutz getroffenen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 Abs. 1 DSGVO.

Leider gibt es in der DSGVO und im BDSG (neu) keine Aufstellung der Gebote mehr, wie sie im „alten“ BDSG im § 9 und der Anlage zu § 9 Satz 1 vorhanden waren. Trotzdem kann man diese oder die im BDSG (neu) im § 64 genannten 14 Gebote als Dokumentationshilfe heranziehen. Wenn die TOMs für mehrere Verfahren bzw. Prozesse gelten ist es klug, diese separat zu dokumentieren und an dieser Stelle darauf hinzuweisen.

Datenschutzfolgeabschätzung:

Birgt eine Verarbeitung besondere Risiken für Rechte und Freiheiten natürlicher Personen, führt der Verantwortliche und der Auftragsverarbeiter vorab eine Abschätzung der Folgen der Verarbeitung durch (Datenschutzfolgeabschätzung). Die Datenschutzfolgeabschätzung gem. Art. 35 DSGVO ersetzt die Vorabkontrolle aus dem "alten" BDSG und muss immer dann durchgeführt werden, wenn sensible Daten bzw. besondere Daten verarbeitet werden (Gesundheitsdaten, Scoring, Profiling, Videoüberwachung etc.). Die Datenschutzfolgeabschätzung setzt sinnigerweise auf dem Verzeichnis der Verarbeitungstätigkeiten auf. Hier müssen die einzelnen Prozesse auf Datensparsamkeit, Integrität, Intervenierbarkeit, nicht Verkettbarkeit, Transparenz, Verfügbarkeit und Vertraulichkeit geprüft und bewertet werden. Und dies sowohl auf Ebene der Daten, auf der Hard- und Softwareebene und der Prozessebene. Ferner sind die Risiken für die von der Verarbeitung betroffenen Personen zu gewichten und auch die Eintrittswahrscheinlichkeit von Fehlern oder möglichen Pannen (z. B. der Versand einer Rechnung an einen falschen Betroffenen). Es ist wie ein Risikomanagement für Datenschutz. Der für die Verarbeitung Verantwortliche holt sich ggf. Rat beim Datenschutzbeauftragten. Auch sollte man für jeden Prozess eine Datenschutzfolgeabschätzung durchführen und diese dokumentieren, auch wenn das Ergebnis voraussichtlich bedeutet, dass keine Datenschutzfolgeabschätzung nötig ist.

Ein Muster einer der Aufsichtsbehörden, wie genau man eine Datenschutzfolgeabschätzung vornimmt, gibt es zur Zeit leider noch nicht. Auch die Verbände halten sich zur Zeit noch mit konkreten Aussagen zurück. Ein Lösungsvorschlag bietet evtl. das Standard Datenschutzmodell, welches von den Aufsichtsbehörden entwickelt wurde.

Schutz-ziel:	Daten	Systeme (Hard- und Software)	Prozesse
Datenspar-samkeit	✔ Nur die Daten die für die Verarbeitung notwendig sind ✔ Begrenzung ✔ Trennung / Zusammenführung	✔ Reduzierung von Verarbeitungen ✔ Sperrung / Löschung ✔ Pseudo- / Anonymisierung	✔ Beschränkung Berechtigter ✔ Löschprozesse ✔ PDCA Prozesse ✔ Kontrollprozesse
Integrität	✔ Protokollierung ✔ Hashes ✔ Berechtigungskonzept	✔ Automatisierte Fehlermeldungen ✔ Berechtigungskonzept ✔ Prüfungen / Tests	✔ Berechtigungskonzept ✔ Rollenkonzept ✔ Prozessfehlermeldungen
Intervenier-barkeit	✔ Schaffung notwendiger Datenfelder	✔ Änderbarkeit ✔ Steuerbarkeit	✔ Änderbarkeit ✔ Protokollierung von Eingriffen ✔ Ticketsystem
Nicht Ver-kettbarkeit	✔ Mandantentrennung ✔ Festlegung von Trennungsmerkmalen	✔ Trennung von Systemen (logisch und physikalisch) ✔	✔ Berechtigungskonzept ✔ Rollenkonzept ✔ Identitäten ✔ Kontrollprozesse
Trans-parenz	✔ Dokumentation der verarbeiteten Daten ✔ Erforderlichkeit	✔ Dokumentation der logischen und physischen Systeme	✔ Dokumentation ✔ Versionierung ✔ PDCA Verfahren
Verfüg-barkeit	✔ Datensicherung	✔ Schutz der Systeme (Antivirus, Firewall, VPN, physischer Schutz, USV etc.)	✔ Notfallhandbücher ✔ Notfallübungen ✔ Tests ✔ Überwachung
Vertrau-lichkeit	✔ Berechtigungskonzept ✔ Protokollierung ✔ Verschlüsselung	✔ Berechtigungskonzept ✔ Protokollierung	✔ Berechtigungskonzept ✔ Rollenkonzept

Gegebenenfalls holt der für die Verarbeitung Verantwortliche zur geplanten Verarbeitung den Standpunkt der von der Verarbeitung betroffenen Personen ein. Dies muss er unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge tun.

Kommt ein Verantwortlicher nach einer Datenschutzfolgeabschätzung zu dem Schluss, dass bei der Verarbeitung trotz Eindämmung des Risikos durch technische und organisatorische Maßnahmen ein hohes Risiko für die betroffenen Personen besteht, hat er gem. Art. 36 DSGVO die Aufsichtsbehörde zu konsultieren.

Merke:
Datenschutzfolgeabschätzung , Sicherheit bei der Verarbeitung, Verzeichnis der Verarbeitungstätigkeiten, technische und organisatorische Maßnahmen sind zu dokumentieren.
Die Integration in ein Managementsystem ist von enormem Vorteil, da sich Bereiche wie Datenschutz, Qualitätsmanagement, Risikomanagement und Compliance überschneiden. Somit können Synergien genutzt werden.

Sicherheit bei der Verarbeitung:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art und Umfang der Verarbeitung, der Eintrittswahrscheinlichkeit und des Risikos für die Betroffenen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete TOMs, um das Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO). Die Vorgaben des BSI an den Stand der Technik sind insbesondere bei der Verarbeitung von Kategorien besonderer Daten (z. B. Gesundheitsdaten) zu beachten.

Maßnahmen können sein:

- Pseodonymisierung und Verschlüsselung (Art. 32 Abs. 1a DSGVO).
- Die Fähigkeit Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme auf Dauer sicherzustellen (Art. 32 Abs. 1b DSGVO).
- Die Fähigkeit die Verfügbarkeit der Daten nach einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1c DSGVO).
- Ein Verfahren zur regelmäßigen Evaluierung der TOMs zur Gewährleistung der Sicherheit bei der Verarbeitung (Art. 32 Abs. 1d DSGVO).
- Die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO kann als Faktor für den Nachweis herangezogen werden (Stichwort: DIN 27001).

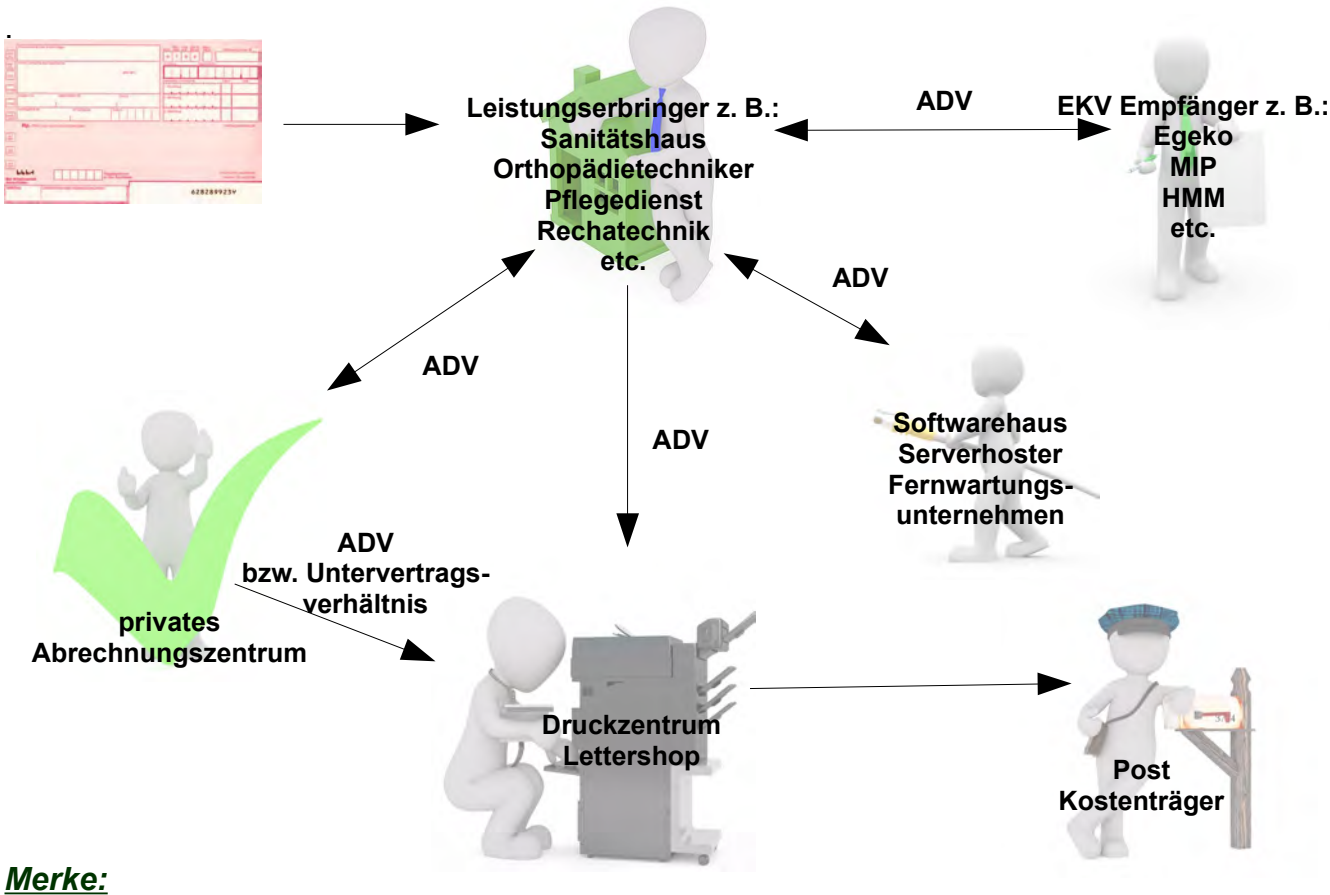
Wie schon beim „Verzeichnis der Verarbeitungstätigkeiten“ beschrieben, gibt es für die Dokumentation der technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) keine Vorgaben mehr wie im „alten“ BDSG unter § 9 und der Anlage zu § 9 Satz 1. Die TOMs im BDSG (neu) sind unter § 64 Abs. 3 definiert. Dieser gilt aber nur für Justizbehörden, Strafvollzug und Ermittlungsbehörden (öffentliche Stellen). Trotzdem eignen sich die 14 Punkte als Dokumentationsgrundlage für die eigenen TOMs. Hinweise was unter den einzelnen Punkten zu dokumentieren ist, finden sich ausreichend im Internet oder auf den Webseiten der Aufsichtsbehörden.

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Auftragsverarbeitung:

Werden Daten zu einem bestimmten Zweck an einen Auftragnehmer (Auftragsverarbeiter nach DSGVO) weitergegeben (outsourcing), kommt häufig eine Auftragsdatenverarbeitung (Auftragsverarbeitung nach DSGVO) zum Einsatz. Beispiele hierfür sind die Weitergabe von Rezepten, Verordnungen, Leistungsnachweisen oder anderen abrechnungsbegründenden Unterlagen an ein Rechenzentrum zum Zweck der Abrechnung und des Datenträgeraustausches mit den Kostenträgern. Aber auch das Serverhosting und die Fernwartung einer Branchenlösung, das Übermitteln von elektronischen Kostenvoranschlägen etc. sind Auftragsdatenverarbeitungen gem. Art. 28 und 29 DSGVO.
Hier müssen spezielle Verträge geschlossen werden und der Auftragsverarbeiter muss hinreichende Garantien bieten und technische und organisatorische Maßnahmen treffen, um die Verarbeitung sicher zu stellen. Er darf ohne die Zustimmung des Auftraggebers keine weiteren Unterauftragnehmer beschäftigen. Er darf die Daten nur nach den Weisungen des Auftraggebers verarbeiten und nutzen und hat dies zu dokumentieren. Auch muss er dafür Sorge tragen, dass alle Mitarbeiter, die mit der Verarbeitung der Daten betraut sind, ausreichend auf den Datenschutz verpflichtet sind. Der Auftraggeber muss überwachen, dass der Auftragsverarbeiter seinen Verpflichtungen nachkommt. Musterverträge für eine Auftragsverarbeitung nach DSGVO befinden sich im Internet auf den Seiten der Verbände und Behörden.

.



Merke:

Es ist zu prüfen (z. B. anhand des Verzeichnisses der Verarbeitungstätigkeiten) an welcher Stelle und für welchen Zweck personenbezogene Daten den Betrieb verlassen. In den meisten Fällen ist dies eine Auftragsverarbeitung. Der Auftraggeber ist dafür zuständig, den Vertrag zu schließen und den Auftragsverarbeiter zu prüfen.

Vernichtung von Datenträgern:

Müssen Datenträger, die nicht mehr benötigt werden, vernichtet werden gibt es ebenfalls bestimmte Regeln. Im Oktober 2012 wurde die Norm DIN 32757-1 durch die ersten beiden Teile der neuen dreiteiligen Norm DIN 66399 (DIN 66399-1 und DIN 66399-2) ersetzt. Seit 2013 hat auch die DIN SPEC 66399-3 Gültigkeit erlangt. Die gegenwärtig noch parallel zur DIN 66399 gültige Europäische Norm EN 15713:2009 weist im Vergleich zur älteren DIN 32757-1 zwar auch einen Materialbezug auf, ist aber zu wenig verbindlich und wird den deutschen Anforderungen von Datenschutz und Informationssicherheit nicht gerecht. Die DIN 66399 entspricht somit dem „Stand der Technik“ und kann als verbindlich angesehen werden.

Unter Datenträger versteht man nicht nur „elektronische bzw. magnetische“ Datenträger wie Festplatten, USB-Sticks, Bänder etc. sondern auch optische Datenträger wie CDs und DVDs und natürlich auch Papier. Unter Bin Raiding versteht man das systematische Durchsuchen von Papiermüll nach verwertbaren Informationen.

In der DIN 66399 wird die datenschutzgerechte Vernichtung von Datenträgern geregelt. Die DIN 66399-1regelt die Grundlagen und Begriffe, definiert die Schutzklassen und Sicherheitsstufen, die DIN 66399-2 definiert die Anforderung an Maschinen, die zur Vernichtung eingesetzt werden, die DIN 66399-3 regelt den Prozess der Vernichtung. Es gibt 3 Schutzklassen, 6 Materialklassifizierungen und 7 Sicherheitsstufen. Gesundheitsdaten werden beispielsweise in die Schutzklasse 3 einsortiert. Handelt es sich um Daten in Papierform ist die Materialklasse P. Werden z. B. nicht mehr benötigte Papierunterlagen vernichtet, auf denen auch Gesundheitsdaten stehen, ist die Sicherheitsstufe mindestens P-4. P-4 bedeutet: Materialteilchenfläche ≤ 160 mm² und für regelmäßige Partikel eine Streifenbreite ≤ 6 mm. Zudem ist noch ein Toleranzbereich angegeben.

Merke:
Die Vernichtung nicht mehr benötigter Datenträger egal ob in Papierform oder auf anderen „Medien“ muss entsprechend der DIN 66399 erfolgen. Werden Datenträger über einen Entsorgungsbetrieb vernichtet ist darauf zu achten, dass dieser die Vernichtung nach DIN 66399 garantiert und auch einhält.

Meldepflicht bei Datenschutzpannen und Datenschutzverstößen:

Führt die Datenschutzpanne zu einem Risiko für die Rechte und Freiheiten eines Betroffenen oder besteht eine Gefahr für die Rechtsgüter einer natürlichen Person ist die zuständige Aufsichtsbehörde innerhalb von 72 Stunden nach bekannt werden des Vorfalls zu informieren (Art. 33 Abs. 1 DSGVO). Zur Feststellung ob ein Vorfall meldepflichtig ist oder nicht, ist es ratsam sich die Meinung des Datenschutzbeauftragten einzuholen und diesen in den Vorfall zu involvieren.

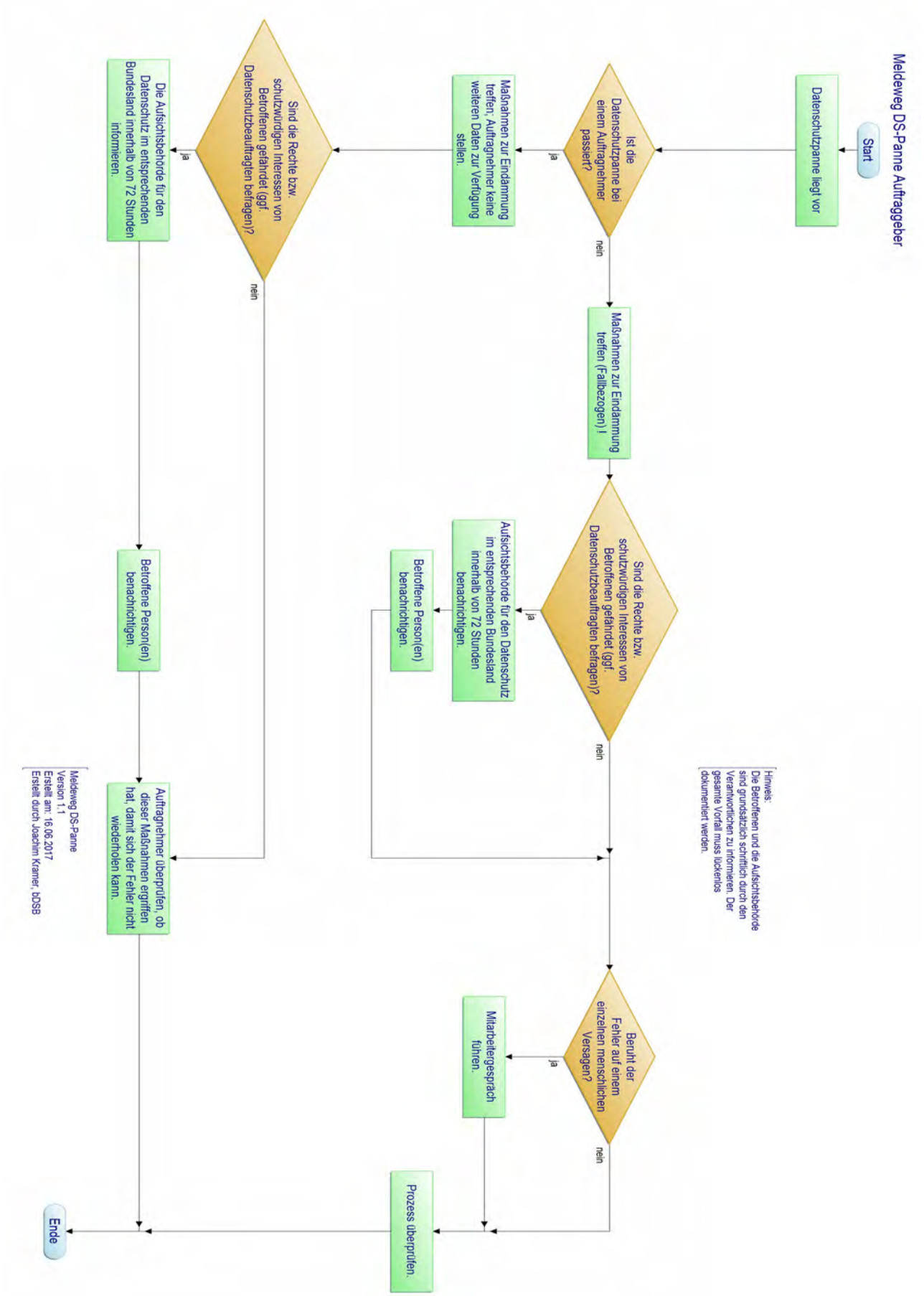
Passiert bei einem Auftragsverarbeiter eine Datenschutzpanne (unabhängig davon ob diese gegenüber der Aufsichtsbehörde meldepflichtig wäre oder nicht) hat er seinen Auftraggeber davon unverzüglich zu unterrichten (Art. 33 Abs. 2 DSGVO).

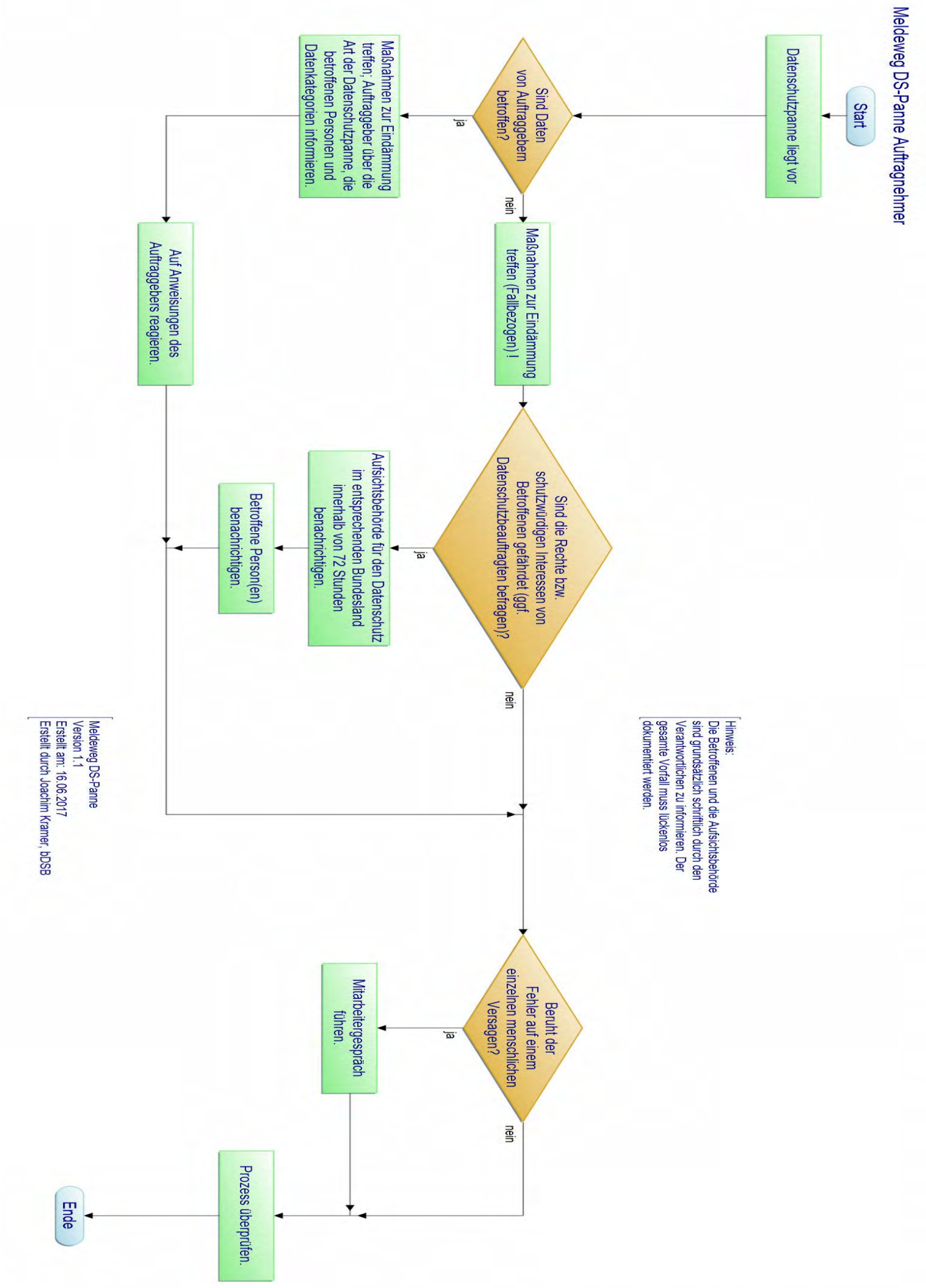
Ferner muss in den oben genannten Fällen der Verantwortliche die von der Datenschutzpanne betroffenen Personen informieren (Art. 34 Abs. 1 DSGVO). Dies kann unter Umständen eine große Anzahl von Betroffenen sein. Z. B.: wird ein Laptop gestohlen, auf dem sich personenbezogene Daten und Gesundheitsdaten befinden und ist dieser Laptop nicht verschlüsselt (was nach einer Datenschutzfolgeabschätzung eigentlich nicht sein kann), muss die Aufsichtsbehörde und die betroffenen Personen informiert werden. Sind es nur 10 Betroffene kann man diese sicherlich einzeln informieren. Ist es aber z. B. der gesamte Kundenbestand von 5000 Betroffenen können diese nicht mehr einzeln informiert werden. In diesen Fällen muss die Öffentlichkeit informiert werden und die Aufsichtsbehörde kann entscheiden, wie dies zu geschehen hat.

Der Inhalt der Meldung ist klar definiert (Art. 33 Abs. 3 DSGVO).

Auch hier ist es sinnvoll einen Prozess zu etablieren wie man mit Datenschutzpannen umgeht. Je ein Beispielprozess aus der Sicht des Auftraggebers (Verantwortlicher) und des Auftragnehmers (Auftragsverarbeiters) befinden sich auf den nächsten Seiten:

Merke:
Der Meldepflicht ist unbedingt nachzukommen. Werden Datenschutzpannen bzw. Verstöße nicht gemeldet und werden diese den Aufsichtsbehörden bekannt drohen empfindlich hohe Bußgelder.





Kompetenzen der Aufsichtsbehörden / Bußgelder:

- sie dürfen anlassfreie Kontrollen durchführen
- sie haben volle Zutritts- und Kontrollrechte
- sie können einzelne Verfahren, die nicht datenschutzkonform sind, verbieten
- sie kontrollieren ob die Betroffenen bei Datenschutzverstößen unterrichtet wurden
- sie haben das Recht Unternehmen zu schließen, wenn angeordnete Nachfristen nicht eingehalten werden
- sie können den Datenschutzbeauftragten abberufen, wenn dieser nicht qualifiziert ist oder seinen Aufgaben nicht nachkommt
- sie erteilen Bußgelder
- sie bestimmen die Höhe die Bußgelds
- sie können Zwangsgelder verhängen
- die Aufsichtsbehörde hat Strafantragsrecht, wenn Verstöße vor Gericht verhandelt werden sollen oder müssen

Bei Verstößen können, je nachdem gegen welchen Artikel der DSGVO verstoßen wurde, Bußgelder in Höhe von bis zu 10.000.000 € bzw. bis zu 20.000.000 € oder 2% bzw. 4% vom weltweiten Jahresumsatz der Unternehmensgruppe erhoben werden, je nachdem welcher Betrag höher ist (Art. 83 DSGVO und § 43 BDSG (neu)).

Die Aufsichtsbehörde stellt sicher, dass die Strafe in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Auch sind Strafen für Auftragnehmer (Auftragsverarbeiter) vorgesehen, wenn diese gegen ihren Auftrag verstoßen oder es zu Datenschutzpannen kommt.

Merke:
Nicht nur die Bußgelder sind in schwindelerregende Höhen gestiegen, vor allem der drohende Imageverlust kann ein Unternehmen in den Konkurs treiben.

Webseitenbetreiber aufgepasst:

Betreiber von Webseiten (wer ist das nicht?) müssen eine Vielzahl an Vorschriften beachten. Regelungen zur "rechtskonformen" Website finden sich u. a. in den §§ 11 ff. Telemediengesetz (TMG) und im § 13 TMG, die die Pflichten des Diensteanbieters vorgeben. Die Datenschutz-Grundverordnung hat Auswirkungen auf die aktuellen Anforderungen an Website-Compliance.

So ist zu prüfen ob das Impressum den rechtlichen Regelungen entspricht, ob es Datenschutzklauseln gibt (Achtung beim Einsatz von Cookies und Analysetools wie z. B. google analytics), ob die Kontaktdaten des Datenschutzbeauftragten veröffentlicht wurden. Wenn es ein Kontaktformular gibt und je nachdem welche Daten mit übertragen werden können müssen die Datenschutzklausel und das Transparenzgebot stimmig sein. Ferner hat die Übertragung der personenbezogenen Daten verschlüsselt zu erfolgen. Für Webshop-Betreiber gibt es weitere zahlreiche Pflichten.

Nach einem Urteil des Oberlandesgerichts Hamburg vom 27.06. 2013 (Az. 3 u 26/12) ist eine Datenschutzerklärung abmahnfähig, wenn sie nicht als einzelner Punkt auf der Homepage aufgeführt ist. Grund für das Urteil des OLG ist, dass nach § 13 Absatz 1, Satz 1 TMG, Nutzer einer Webseite zu Beginn des Nutzungsvorgangs über Zweck, Art und Umfang der Erhebung und Verwendung personenbezogener Daten unterrichtet werden. Der Nutzer muss jederzeit den Inhalt der Unterrichtung zur Datenerhebung direkt abrufen können.

Vorsicht auch beim Einsatz von Facebook Buttons auf der Website. Gibt es einen Link zu Facebook und muss der Nutzer aktiv klicken, um zu Facebook zu gelangen, gibt es kaum ein Problem, sofern in der Datenschutzerklärung darauf hingewiesen wird. Wird aber ein so genanntes "Plugin" auf der Website integriert bekommt ein Nutzer gar nicht mit, dass seine Daten (IP-Adresse etc.) an Facebook übermittelt werden. Hier handelt es sich dann um eine nicht statthafte Übermittlung von personenbezogenen Daten (IP-Adresse) in ein Drittland.

Merke:
Die Website ist genau zu prüfen. Viele Anwaltskanzleien haben sich auf Abmahnen eines nicht gesetzeskonformen Internetauftritts spezialisiert. Lassen Sie ggf. Ihre Website durch einen externen Dienstleister auf Rechtskonformität überprüfen.

Hinweise / Links / Nützliches:

Im Internet gibt es zahlreiche Hinweise, Muster und Artikel zu allen Themen des Datenschutzes. Diese sind mehr oder weniger gut bzw. aufschlussreich. Gute Hinweise, Tipps und Arbeitsmaterial findet man bei den Aufsichtsbehörden für den Datenschutz der einzelnen Länder sowie bei der Bundesbeauftragten für den Datenschutz. Die großen Verbände bieten ebenfalls eine gute Basis für eine Recherche zu einem bestimmten Thema. Einige Links sind hier aufgeführt.

https://www.ldi.nrw.de/	*Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Aufsichtsbehörde in NRW – stellvertretend hier für die anderen 15 Aufsichtsbehörden genannt)*
https://www.bfdi.bund.de/	*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*
https://www.bsi.bund.de/	*Bundesamt für Sicherheit in der Informationstechnik*
https://www.gdd.de/	*Gesellschaft für Datenschutz und Datensicherheit e.V.*
https://www.bvdnet.de/	*Berufsverband der Datenschutzbeauftragten Deutschlands e.V.*
https://www.sicher-im-netz.de	*Deutschland sicher im Netz e.V.*

Es gibt zahlreiche weitere gute Webseiten wo Datenschutzbeauftragte fündig werden können. Bei den oben genannten Webseiten kann man relativ sicher sein, dass die dort getätigten Aussagen, Arbeitshilfen und Muster rechtskonform sind.

Quellennachweise:

EU-Datenschutzgrundverordnung (DSGVO)	(Verordnung EU 2016/679)
Bundesdatenschutzgesetz (BDSG (neu))	(Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU))
Bilder	www.pixabay.com

erstellt durch:

Kramer & Partner GbR
Dipl-Ing. (FH) Sylvia Kramer und Joachim Kramer
Büro für Datenschutz und Datensicherheit
Elsternweg 24
42555 Velbert

in Kooperation mit der:

ZMT e.V.
Zentralvereinigung medizin-technischer Fachhändler,
Hersteller, Dienstleister und Berater
Hugo-Junkers-Straße 22
50739 Köln