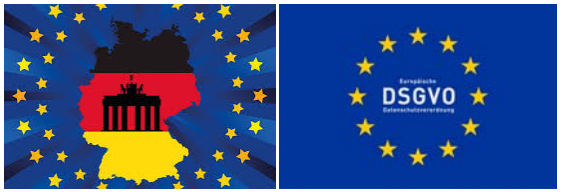
Datenschutz nach dem Bundesdatenschutzgesetz (neu) und der EU-Datenschutz-Grundverordnung

Dresden, 21.06.2018

Dr. Thomas Pudelko
Datenschutzbeauftragter

Dachverband Gemeindepsychiatrie e.V.

Überblick



- Zentrale Elemente des Datenschutzes
- Die Verordnung (EU) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) **EU-DSGVO**
  und das
- Datenschutz - Anpassungs- und Umsetzungsgesetz EU – (**DSAnpUG-EU**)
  sowie das
- Bundesdatenschutzgesetz (**BDSG**) *neu*
- Verortung dieser Elemente in der Organisation
- Sanktionen und Bußgelder

Dachverband Gemeindepsychiatrie e.V.

Was unter Verarbeitung von Daten zu verstehen ist

Dachverband Gemeindepsychiatrie e.V.

Leitmaxime des Datenschutzes

Nur die Informationen über eine Person sammeln, die für die Durchführung der Arbeit notwendig sind (**Erforderlichkeit**)

Informationen nur für den Zweck verwenden, für die sie erhoben wurden (**Zweckbindung**)

Die Daten allen Dritten ggü. verschlossen halten; gegenüber den Betroffenen jedoch offenbaren welche Daten wofür wie und wo wie lange gespeichert werden (**Transparenz**)

Dachverband Gemeindepsychiatrie e.V.

Leitmaxime des Datenschutzes
Datenvermeidung

Ist die Erhebung der Daten notwendig?

Ist die Erfassung der Daten notwendig?

Was passiert, wenn nicht?

Wie lange muss gespeichert werden?

Ist die Löschung gewährleistet?

Leitmaxime des Datenschutzes
Datenerhebung

Daten sind grundsätzlich bei den Betroffenen zu erheben

Der/die Betroffene ist über
- die Rechtsgrundlagen der Erhebung,
- den Erhebungszweck und
- den Zweck der Verarbeitung
- die Dauer der Speicherung

aufzuklären

Dachverband Gemeindepsychiatrie e.V.

Leitmaxime des Datenschutzes
Datenspeicherung

Daten sollten nur dann gespeichert werden, wenn dies für die konkrete Aufgabenerfüllung aktuell erforderlich ist.

Unter Datenspeicherung wird auch das Festhalten von Information in Akten oder anderer schriftlicher Weise verstanden.

Dachverband Gemeindepsychiatrie e.V.

Leitmaxime des Datenschutzes
Datennutzung (Zweckbindung)

Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden.
Z.B.

- Behandlung / Therapie
- Veranstaltung
- Ausbildung
- Rundmail
- Infoverteiler
- Spenderliste

etc.

Dachverband Gemeindepsychiatrie e.V.

Leitmaxime des Datenschutzes
Einwilligung der Betroffenen

Eine Übermittlung an Dritte ist immer dann zulässig, wenn der Betroffene eingewilligt hat.

„Betroffener“ ist derjenige, um dessen Daten es geht.

Die Einwilligung muss sich auf konkrete Informationen beziehen, kann also nicht pauschal gegeben werden.

Leitmaxime des Datenschutzes
Gesteigerter Schutz

In besonderen Fällen, wenn Mitarbeitern Informationen aufgrund einer besonderen persönlichen Vertrauensbeziehung anvertraut wurden, genießen diese gesteigerten Schutz (z.B. Therapeutisches Verhältnis)

Diese Bestimmung (§ 65 SGB VIII) geht allen anderen vor, die sonst eine Weitergabe rechtfertigen würden, auch z.B. der Mitteilungspflicht nach § 138 StGB

Zentrale Elemente der EU-DSGVO

- Datenschutz – Leitlinien (Management/Verantwortlichkeiten)
- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutzfolgeabschätzung (Prozess)
- Zuständigkeiten für Datenschutz (DSB) (Verträge)
- Externe Datenverarbeitung (Auftragsdatenverarbeitung) (Prozess)
- Information der Personen, deren Daten erhoben werden (Verfahren)
- Auskunftsfähigkeit über Verarbeitungstätigkeiten (Prozess)
- Verfahren zur Überprüfung der Datensicherheit (Audit)
- Verfahren zum Umgang mit Datenschutzunfällen (Prozess)
- Regeln zur Schulung von Mitarbeiter_inen/Mitgliedern in DS-Fragen

Weitere Elemente der EU-DSGVO

- Die Sicherheit der Daten muss durch geeignete technische Maßnahmen gewährleistet werden (IT)
- Beschäftigtendatenverarbeitung (Management/Verantwortlichkeiten)
- Recht auf Berichtigung (Management/Verantwortlichkeiten)
- Recht auf Löschen (Management/Verantwortlichkeiten)
- Recht auf Datenübertragbarkeit (Management/Verantwortlichkeiten)
- Automatisierte Entscheidungen
- DV zu wissenschaftlichen und statistischen Zwecken
- Zusammenarbeit der Datenschutzbehörden, Aufsicht
- Bußgelder (Management/Verantwortlichkeiten)

Dachverband Gemeindepsychiatrie e.V.

Datenschutz – Leitlinien
(Management/Verantwortlichkeiten)

Festlegung von Zuständigkeiten
- in der Gesamtorganisation
- in den Teilorganisationen
- auf allen Ebenen

Dies bedeutet:

- In jeder Organisationseinheit (Abteilung, Bereich, Team, Standort etc.) sind Personen zu benennen, die in ihrer Zuständigkeit auf DS und IT- Sicherheitsaspekte zu achten haben.
- Die Aspekte zur Sicherheit der Verarbeitung personenbezogener Daten (Art. 32 EU – DSGVO) sind für die IT in der Organisation verbindlich zu regeln.
- Die Technikgestaltung der IT der Software ist datenschutzfreundlich zu gestalten und in einer DS – Leitlinie zu regeln

Dachverband Gemeindepsychiatrie e.V.

Verzeichnis der Verarbeitungstätigkeiten

Bisher: Internes Verfahrensverzeichnis
Änderungen zu den Anforderungen aus dem BDSG (alt)

- Es ist kein öffentliches Verfahrensverzeichnis mehr gefordert
  inwieweit das neue Verzeichnis nach außen sichtbar sein soll, ist unklar
- Die Bezüge zur nun gültigen Rechtsquelle (Art. 30 EU-DSGVO, § 70 BDSG neu) muss auf allen Dokumenten deutlich sein.
- Die einzelnen erfassten Verfahren müssen die in Art. 30 EU-DSGVO geforderten Kategorien enthalten.
  Die besonderen Kategorien personenbezogenen Daten (Art. 9 EU-DSGVO) (rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit) sind um Gesundheitsdaten, Sexualleben oder sexuelle Orientierung, genetische und biometrische Daten ergänzt worden.
  Gleiches gilt für Daten über strafrechtliche Verurteilungen oder damit zusammenhängende Maßnahmen.
- Besteht bereits ein (altes) internes Verfahrensverzeichnis, muss dieses angepasst werden.

Dachverband Gemeindepsychiatrie e.V.

Datenschutz - Folgeabschätzung (DSB) (Prozess)

In der Organisation ist ein Verfahren zu installieren, dass sicher stellt, dass im Falle eines neuen
Verfahrens/Vorganges/Geschäftsgange/Softwareeinführung etc.
bei dem personenbezogene Daten
erhoben, erfasst, geordnet, gespeichert, angepasst, verändert, ausgelesen, abgefragt, offengelegt, übermittelt, verbreitet, gelöscht, oder vernichtet werden sollen, die Rechte der entsprechenden Personen gewahrt werden, wenn dabei ein hohes Risiko besteht.*
Hat die Organisation einen Datenschutzbeauftragten, so ist die Entsprechende Folgeabschätzung durch diese/n vorzunehmen.
(Art. 35, 36 EU – DSGVO)
Ansonsten ist die Aufsichtsbehörde zu konsultieren.

* Die Aufsichtsbehörde soll gem. Art. 35, Abs. 4 und 5 eine Liste von solchen Verarbeitungstätigkeiten erstellen.

Dachverband Gemeindepsychiatrie e.V.

Zuständigkeiten für Datenschutz (DSB) (Verträge)

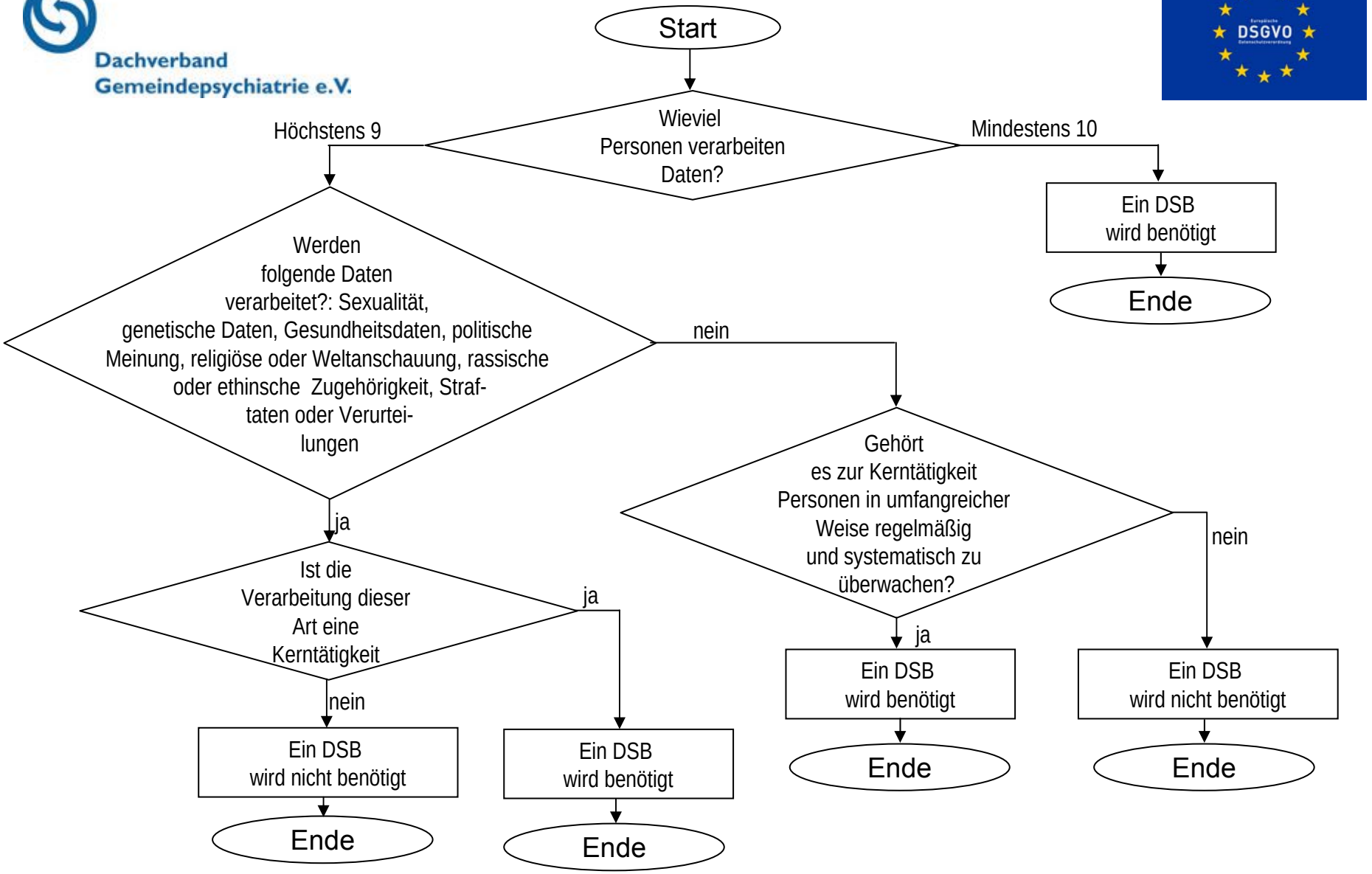
In Organisationen ist die oberste Leitung auch für die Einhaltung von Datenschutzbestimmungen verantwortlich.
Die Leitung kann für die Überwachung etc. der Datenschutzbestimmungen in der jeweiligen Organisation einen Datenschutzbeauftragten (DSB) bestellen.
In bestimmten Fällen ist die Bestellung eines DSB vorgeschrieben.

- Wenn es zur Kerntätigkeit der Organisation gehört Daten gemäß Art. 9 EU – DSGVO zu verarbeiten,
- Wenn Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden.*

Eine Unternehmensgruppe darf einen gemeinsamen DSB ernennen.

* Hierzu gehören z.B. auch die Informationen aus den erweiterten Führungszeugnissen, von z.B. Mitarbeitern, die mit Kindern oder Jugendlichen arbeiten

Dachverband Gemeindepsychiatrie e.V.



Dachverband Gemeindepsychiatrie e.V.

Aufgaben eines Datenschutzbeauftragten

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten von Datenschutzvorschriften;
- Überwachung der Einhaltung der einschlägigen Datenschutzvorschriften
- Überwachung der Strategien des Verantwortlichen beim Einhalten von Schutzvorschriften personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten,
- Sensibilisierung und Schulung der MitarbeiterInnen
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit Datenschutz zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.
- Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Dachverband Gemeindepsychiatrie e.V.

Externe Datenverarbeitung Auftragsdatenverarbeitung)

- Erfolgt die Datenverarbeitung durch Dritte, so hat der Auftraggeber durch
  Vertragsgestaltung dafür Sorge zu tragen, dass der Auftragnehmer die
  Bestimmungen aus der EU –DSGVO und dem EU – DSAnpUG-EU einhält. (Art. 28 EU – DSGVO)
- Gibt der Datenverarbeitungsauftragnehmer wiederum einen Auftragsdatenverarbeiter den Auftrag oder einen Teil davon weiter, so ist der Auftraggeber darüber und über die Inhalte darüber zu informieren. Auch der Unterdatenverarbeitungsauftragnehmer muss die Einhaltung der entsprechenden Vorschriften nachweisen.
- Erlässt die EU in Folge hierzu noch Standardvertragsklauseln, so sind die bisher hierzu geschlossenen Verträge anzupassen. (Art. 28, Abs. 7 EU – DSGVO)

Dachverband Gemeindepsychiatrie e.V.

Information der Personen, deren Daten erhoben werden

- Die betroffene Person muss über die sie betreffenden Daten informiert werden. (Art. 6, 7, 14 EU-DSGVO)
- Bei der Erfassung personenbezogener Daten muss die zu erfassende Person
  - über den Zweck informiert,
  - über die Gründer der Erfassung aufgeklärt,
  - die Art und Weise der Speicherung, Verarbeitung, Löschung informiert
  - erfahren, dass die Person das Recht hat auch nachträglich die Löschung ihrer Daten verlangen zu können (vorbehaltlich vertraglicher Verpflichtungen)

  umfassend und in einfacher und verständlicher Sprache informiert werden.
- Die Zustimmungseinholung darf nur für jeweils einen Zweck erfolgen (Verbot der konkludierenden Einverständniserklärung)

Dachverband Gemeindepsychiatrie e.V.

Auskunftsfähigkeit über Verarbeitungstätigkeiten

Die Organisation muss ein Verfahren entwickeln, mit dem sie auskunftersuchenden Personen
- schriftlich
- in einer angemessenen Zeit (
- über sie in der Organisation gespeicherte Daten und
- ggf. übermittelte Daten (an wen, warum) an Dritte

Auskunft geben kann. (Art. 12,15 EU – DSGVO)

Diese Auskunft muss alle Datenkategorien umfassen, den Zweck, der Speicherung, Verarbeitung sowie ggf. Empfänger bei Weitergabe in einfacher und verständlicher Sprache und übersichtlich sein.

Dabei muss der auskunftersuchenden Person auch mitgeteilt werden, dass für sie die Möglichkeit besteht, sich bei der Aufsichtsbehörde zu beschweren (Art. 15, 1,f EU – DSGVO)

Dachverband Gemeindepsychiatrie e.V.

Verfahren zur Überprüfung der Datensicherheit (Audit)

Die Organisation muss ein Verfahren entwickeln, mit dem sie
- regelmäßig
- den Zustand der Datensicherheit
- des Datenschutzes

und die
- Erfüllung der damit verbundenen Auflagen

intern überprüfen kann.
(Dies sollte in Form eines Audits geschehen.
Diese Aufgabe sollte in Kooperation von
- Datenschutzbeauftragtem

und
- einer weiteren von der Leitung beauftragten Person

geschehen

Dachverband Gemeindepsychiatrie e.V.

Verfahren zum Umgang mit Datenschutzunfällen I

Die Organisation muss ein Verfahren festlegen, wie die Auflagen erfüllt werden,
- wie eine Verletzung „des Schutzes personenbezogener Daten“ innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet wird.

Diese Meldung muss bestimmte Informationen zwingend enthalten
- Art der Verletzung,
- Angaben über die Datenkategorien,
- Anzahl der betroffenen Personen,
- Anzahl der Datensätze,
- Name und Kontaktdaten des Datenschutzbeauftragten,
- Folgenbeschreibung für die betroffenen Personen,
- Beschreibung der durch die Organisation ergriffenen Maßnahmen.
- Der Vorgang ist, einschließlich aller damit im Zusammenhang stehender Fakten,
  deren mögliche Auswirkungen,
  der ergriffenen Abhilfemaßnahmen,

zu dokumentieren. (Art. 34 EU – DSGVO, §§ 65, 66 EU – DSAnpUG-EU)

Dachverband Gemeindepsychiatrie e.V.

Verfahren zum Umgang mit Datenschutzunfällen II

Auch die Personen, deren Daten bei einem Datenunfall betroffen sind, und wo „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge“ besteht, müssen diese Personen unverzüglich Darüber informiert werden.
Dese Information muss in einfacher und klarer Sprache erfolgen.
Nicht benachrichtigt müssen die betroffenen Personen, wenn

- die betroffenen Daten verschlüsselt sind,
- durch andere Maßnahmen sichergestellt ist, dass die Rechte der betroffenen Personen „aller Wahrscheinlichkeit nach nicht mehr bestehen“.
- die einzelne Benachrichtigung unverhältnismäßig aufwendig ist. In diesem Fall kann auch eine öffentliche Bekanntmachung, z.B. durch Anzeigen in Tageszeitungen erfolgen.
- Die Aufsichtsbehörde kann die entsprechende Organisation dazu verpflichten die Information der Betroffenen durchzuführen. (Art. 34 EU – DSGVO)

Dachverband Gemeindepsychiatrie e.V.

Regeln zur Schulung von Mitarbeiter_inen/Mitgliedern in DS-Fragen

Zu den Aufgaben der für den Datenschutz in einer Organisation zuständigen Person gehört auch die Unterrichtung der in einer Organisation mit der Verarbeitung beschäftigen Personen zu Fragen der EU-DSGVO sowie sonstigen Datenschutzvorschriften
(§ 4g Art. 39 Abs. 1 lit. b EU – DSGVO)

Dies ist immer dann Aufgabe des Datenschutzbeauftragten (DSB), wenn ein DSB in einer Organisation erforderlich ist.
Ansonsten hat die oberste Leitung für die entsprechende Schulung direkt Sorge zu tragen.

Dachverband Gemeindepsychiatrie e.V.

Verortung im Management

- Aufnahme des Datenschutzes in die grundlegenden Dokumente der Organisation (Geschäftsordnung, Satzung, Konzeption etc.)
- Prozess zur Erstellung/Pflege des Verzeichnisses der Verarbeitungstätigkeiten erarbeiten und in das Organisationshandbuch einpflegen.
- Erstellung einer DS-Leitlinie und Aufnahme dieser in das Organisations-handbuch
- Verträge mit Auftragsdatenverarbeitern anpassen und in das Organi-sationshandbuch übernehmen.
- Ernennung/Beauftragung eine/s/r DSB und dieses der Aufsichtsbehörde mitteilen.
- Prozesse für Datenschutzunfälle, die Bearbeitung von DS-Anfragen und die Vorabprüfung erarbeiten und in das Handbuch einbinden.
- Datenschutzaudits erarbeiten und durchführen.
- Datenschutzschulungen in den Prozess Personalentwicklung einpflegen

Dachverband Gemeindepsychiatrie e.V.

Fragen in der praktischen Umsetzung

- Wie muss eine Datenschutzerklärung auf der Homepage meiner Organisation aussehen?
- Was muss alles wie in dieses Verzeichnis der Verarbeitungstätigkeiten und was passiert dann damit?
- Was gehört in meinem Institut alles zu den TOMS (Technisch-organisatorischen Maßnahmen)?
- Mit wem muss ich alles eine Auftragsdatenvereinbarung abschließen? Wie muss diese aussehen?
- *Datenschutzfolgeabschätzung - wann ist sie notwendig und wie sieht so etwas exemplarisch aus*?
- Wie mit Auskunftersuchen umgehen, wenn zu befürchten ist, dass dahinter eine Abmahnkanziel steckt?
- Muss ich ein Datenschutzaudit machen, auch wenn ich kein QM-Systemn habe? Wie sieht so etwas aus?
- Benötige ich in meinem Institut Datenschutzsicherheitsleitlinien? Wie sieht so etwas exemplarisch aus?
- Muss jede Organisation Datenschutzziele für sich formuliert haben? Wie könnten diese aussehen? Wo müssen diese stehen?

Bußgelder und Strafverfahren

Dachverband Gemeindepsychiatrie e.V.

Bußgelder und Strafverfahren

Die Aufsichtsbehörde ist befugt

- vom Datenverarbeiter alle den DS befindliche Informationen zu verlangen
- Datenschutzüberprüfungen vorzunehmen,
- auf Verstöße hinzuweisen,
- Zugang dafür zu den Geschäftsräumen, den DV-Anlagen und –geräten zu erhalten. (§ 40, Abs. 5 EU – DSAnpUG-EU)

„Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist.“ (Art. 83, Absatz 6, EU – DSGVO)

Dachverband Gemeindepsychiatrie e.V.

Bußgelder und Strafverfahren

Die §§ 42, 43 EU – DSAnpUG-EU bedrohen bestimmte Verstöße sogar mit Freiheitsstrafen bis zu drei Jahren.

Wer wissentlich personenbezogene Daten einer großen Anzahl von Personen
- einem Dritten übermittelt,
- auf andere Art und Weise zugänglich macht,
- und hierbei gewerbsmäßig handelt.

Wer personenbezogene Daten, die nicht allgemein zugänglich sind,
- und nicht dazu berechtigt ist,
- verarbeitet,
- durch unrichtige Angaben erschleicht
- dies gegen Entgelt tut, oder in dieser Absicht handelt,
- oder einen anderen damit schädigt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft.

§ 43 Bußgeldvorschriften

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

der Aufsichtsbehörde ein neues Verfahren, was der Vorabprüfungspflicht unterliegt, nicht meldet,

diese Meldung unvollständig und/oder falsch ist,

einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

Dachverband Gemeindepsychiatrie e.V.

Bußgelder und Strafverfahren

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

bei der Datenübermittlung es an der notwendigen Sorgfalt fehlen lässt,

bei der Auftragsdatenverarbeitung vor Beginn der Datenverarbeitung sich nicht von der Einhaltung der notwendigen technischen und organiatorischen Maßnahmen überzeugt,

bei der Datenverarbeitung für eigene Zwecke der Dateninhaber nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sichergestellt wird, dass der Betroffene Kenntnis erhalten kann,

Über den Zweck der Datenverarbeitung ist der Dateninhaber nicht so unterrichtet, dass dieser den Inhalt versteht,

Dachverband Gemeindepsychiatrie e.V.

Bußgelder und Strafverfahren

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

die Daten zu anderen Zwecken verwendet werden als diese ursprünglich erhoben wurden,

Die Daten, die für einen anderen Zweck zur Verfügung gestellt wurden, in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

die Daten erstmalig ohne das Wissen des Dateninhabers gespeichert werden, und der Dateninhaber darüber nicht umfassend informiert wurden. Geschieht dies nicht, nicht richtig oder nicht vollständig, handelt der Zuständige ordnungswidrig.

Dachverband Gemeindepsychiatrie e.V.

Bußgelder und Strafverfahren

Erteil die zuständige Stelle der nachfragenden Person nicht Auskunft über die über ihn gespeicherte Information, oder ist dese unvollständig oder geschieht dies nicht rechtzeitig.

Ist das Auskunftersuchen an anderer Stelle zu bearbeiten, so muss dies durch die annehmende Stelle sicher gestellt werden.

Die zuständige Stelle muss der Aufsichtsbehörde umfassend, unverzüglich und Auskunft geben. Kontrollen vor Ort müssen geduldet werden.

Anordnungen darf nicht zuwider gehandelt werden.

Dachverband Gemeindepsychiatrie e.V.

Links und Hinweise

- Der Europäische Datenschutzbeauftragte
  https://edps.europa.eu/edps-homepage_de
- Die Datenschutzbeauftragte Deutschland
  https://www.bfdi.bund.de/DE/Home/home_node.html
- Bundesamt für Sicherheit in der Informationstechnik
  https://www.bsi.bund.de/DE/Home/home_node.htm
- Datenschutz - in der Praxis umsetzen
  https://www.datenschutz-praxis.de/fachnews/datenschutz-folgenabschaetzung-wann-und-wie-umsetzen/
- Deutsche Vereinigung für Datenschutz
  https://www.datenschutzverein.de/
- Informationsportal für Datenschutzbeauftragte
  https://www.datenschutzbeauftragter-info.de/
- Dr. Thomas Pudelko datenschutz@t-pudelko.de