Pridatect

WEBINAR

DiGA Zertifizierung und Datenschutz

Lisa Hofmann

Chief of Legal Operations
Pridatect

TÜV zertifizierte
Datenschutzbeauftragte

LinkedIn

Natalya Spuling

Rechtsanwältin und
Datenschutzbeauftragte

Gesundheitsdatenschutz,
Skill Mentor GDPR
#EUvsVirus

LinkedIn

Senden Sie uns Ihre Fragen

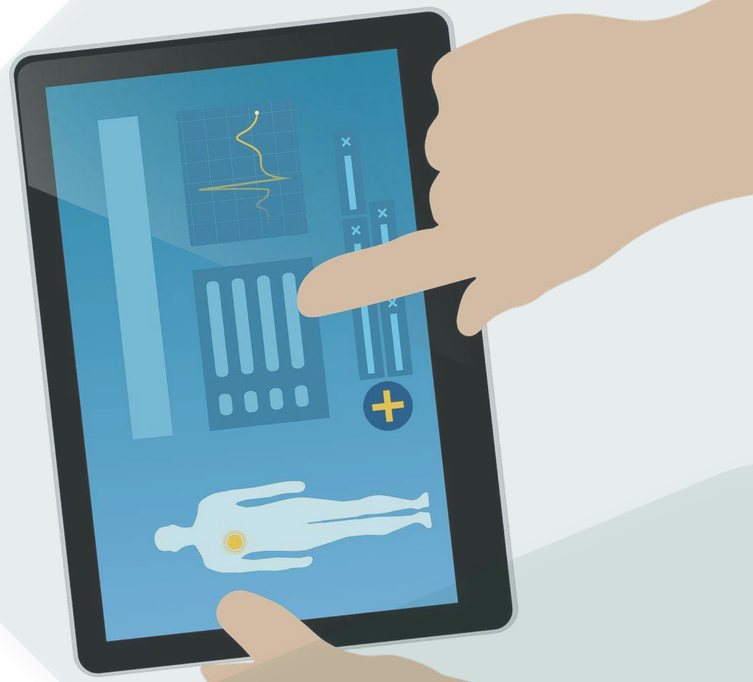
lisa.hofmann@pridatect.com

Digitale Gesundheits-Apps

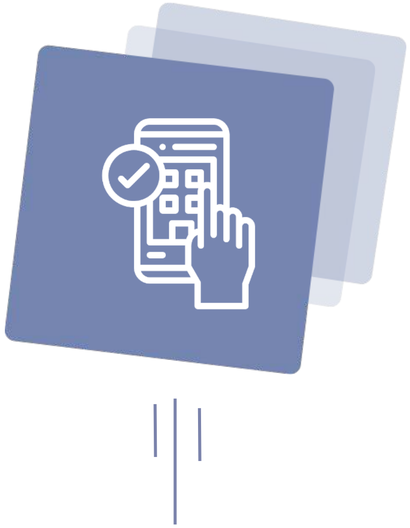
Seit März 2020 ist die **Digitale-Gesundheitsanwendungen-Verordnung** (DiGAV) in Kraft getreten**:** Deutschland führt weltweit als erster Staat **Gesundheits-Apps auf Rezept** ein. Demnach können Kosten für Gesundheits-Apps von Krankenkassen übernommen werden, wenn ein Arzt sie verschreibt.

Über ein Fast Track Verfahren werden Applikationen geprüft und als DiGA zertifiziert. Bisher haben es **5 Gesundheits-Apps** geschafft, alle Anforderungen zu erfüllen und in das **DiGa Verzeichnis** aufgenommen zu werden

Es gibt zahlreiche Gesundheits-Apps, die als DiGAs in Frage kämen. Seit Inkrafttreten der DiGAV vor 9 Monaten haben es nur wenige in das Verzeichnis geschafft. Welche ***Anforderungen und Hürden*** *gibt es bei der Zulassung und beim* ***Fast Track Verfahren?***

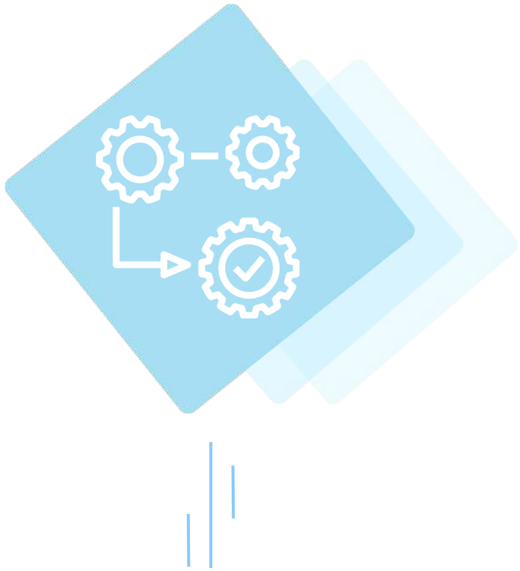


Agenda



Der DiGA Zertifizierungsprozess

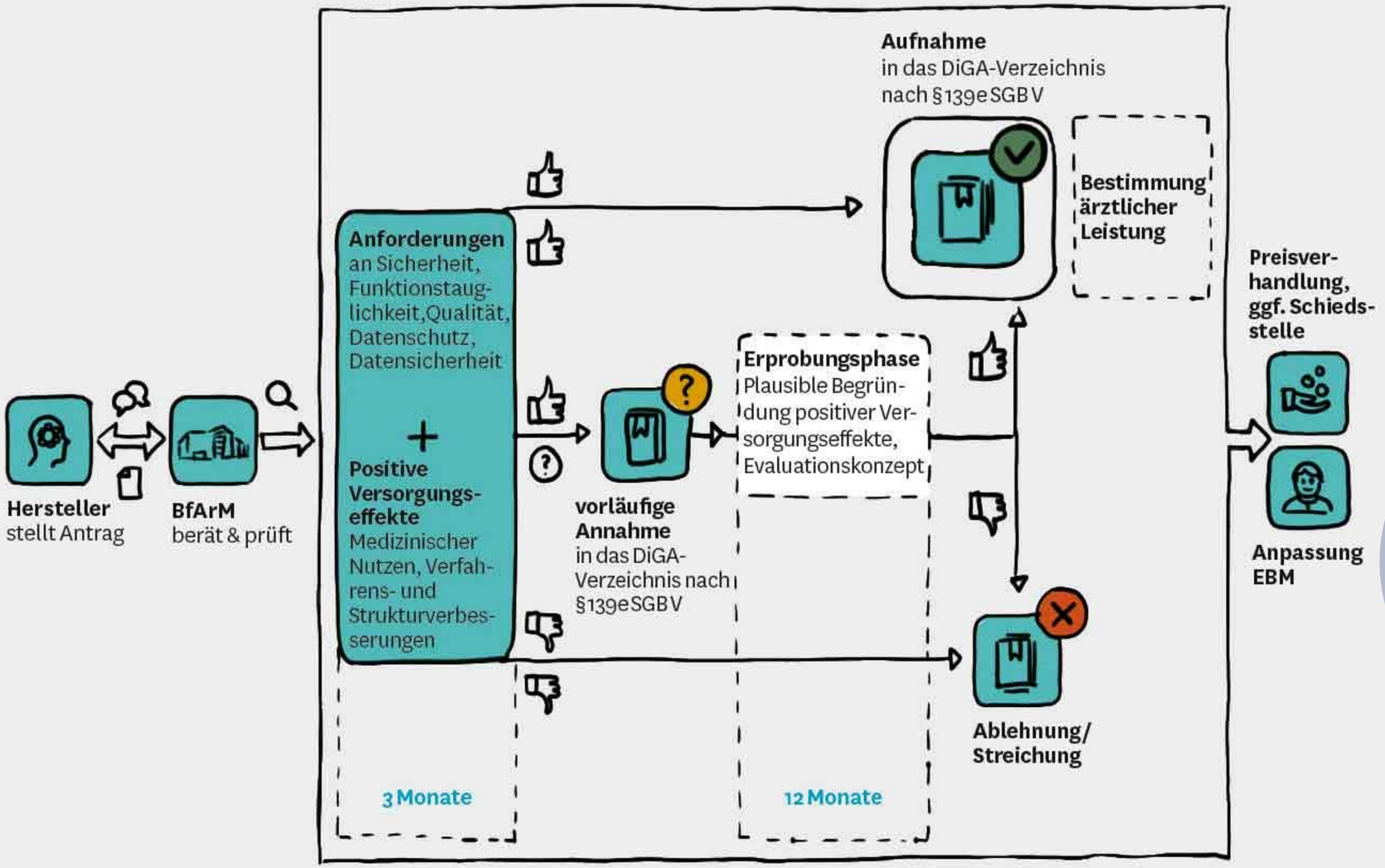
Datenschutz-Anforderungen



Datensicherheit als Prozess

Praktisch gelöst mit Pridatect

Das Fast Track Verfahren zur DiGA Zertifizierung



Quelle: Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)

"Datenschutz und Datensicherheit sind ein essenzieller Bestandteil der Prüfung zur DIGA Zertifizierung."

Anforderungen an eine DiGA

Um im Verzeichnis nach § 139e SGB V gelistet zu werden, muss eine DiGA zunächst die in §§ 3 bis 6 DiGAV definierten Anforderungen erfüllen zu:

Sicherheit und Funktionstauglichkeit

Datenschutz und Informationssicherheit

Qualität, insbesondere Interoperabilität

Grundlage hierzu sind neben dem Nachweis der Erfüllung medizinprodukterechtlicher Anforderungen vor allem die vom Anbieter einer DiGA auszufüllenden **Checklisten**, die in den **Anlagen 1 und 2** der DiGAV aufgeführt sind

Anlage 1: Anforderungen an **Datenschutz und Informationssicherheit**

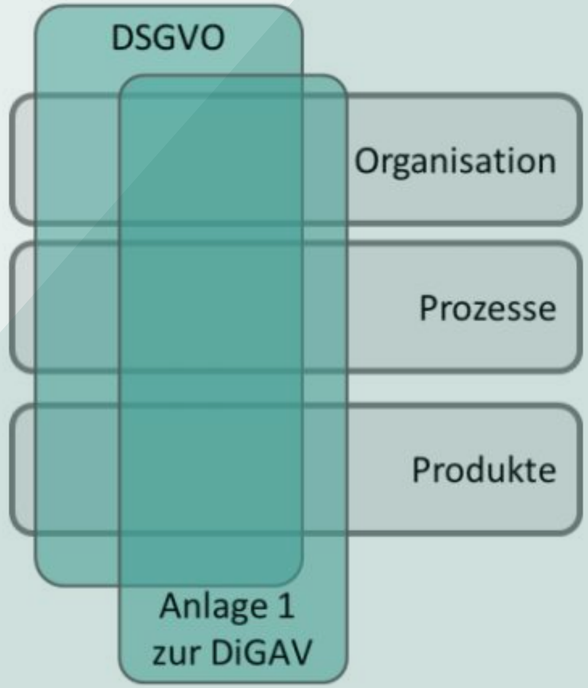
Anlage 2: Anforderungen an **Interoperabilität, Robustheit, Verbraucherschutz, Nutzerfreundlichkeit, Unterstützung von Leistungserbringern, Qualität medizinischer Inhalte und Patientensicherheit**

Der **Datenschutz nach DSGVO** ist Teil der Anforderungen, somit muss dieses Thema **schon vor der Zulassung als DiGA** und Aufnahme in das Verzeichnis sichergestellt werden.

Datenschutz-Anforderungen zur Aufnahme ins DiGA-Verzeichnis

Die DiGAV konkretisiert die Vorgaben aus der Datenschutz-Grundverordnung (DSGVO) und weiterer datenschutzrechtlicher Vorgaben für das Unternehmen des Herstellers, für die **DiGA selbst** und für **alle Systeme in Verbindung** mit der DiGA

- DSGVO & BDSG (Bundesdatenschutzgesetz)
- § 22 BDSG (ggf. i. V. m. Art. 9 DSGVO) als Zentrale Vorschrift für die Verarbeitung von Gesundheitsdaten
- DiGAV Anlage 1: Checkliste mit 40 Aussagen zum Datenschutz
  - **technische Umsetzung** der DiGA (z. B. im Hinblick auf technische und organisatorische Maßnahmen gem. Art. 32 DSGVO)
  - **Organisation des Herstellers**
  - **Unternehmens-Prozesse** (z. B. Sicherstellen einer datenschutzkonformen Zusammenarbeit mit externen Dienstleistern durch Auftragsverarbeitungsverträge)
- Einzelne Vorgaben der DSGVO für den Bereich des Einsatzes digitaler Produkte im Gesundheitswesen werden weiter konkretisiert
  - die zulässigen Zwecke der Datenverarbeitung und
  - die Nicht-Zulässigkeit einer Verarbeitung im Ausland auf Basis von Art. 46 DSGVO.



Anforderungen aus Anlage 1 DiGAV:

Fragebogen mit 40 Fragen gemäß § 4 Absatz 6 der DiGAV.
Die Fragen verteilen sich auf die **folgenden Datenschutzkategorien:**

- Einwilligung
- Zweckbindung
- Datenminimierung & Angemessenheit
- Integrität & Vertraulichkeit
- Richtigkeit
- Erforderlichkeit
- Datenportabilität
- Datenschutzmanagement

- Informationspflichten
- DSFAs & Risikomanagement
- Nachweispflicht
- Auftragsverarbeitung
- Verarbeitung im Ausland
- Weitergabe an Dritte
- Weitere Gewährleistungsziele

Eine in der Anlage 1 oder 2 nicht zur Auswahl vorgegebene „Nicht zutreffend“-Antwort erfordert eine schriftliche Begründung, warum das der Aussage übergeordnete Kriterium dennoch erfüllt wird.

Zulässigen Zwecke der Datenverarbeitung

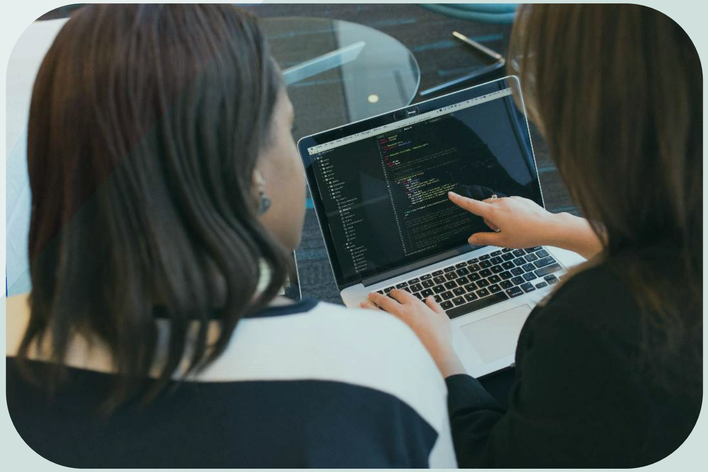
Die Digitale-Gesundheitsanwendungen-Verordnung (DiGaV) stellt spezielle Anforderungen an die Anbieter von digitalen Anwendungen (DiGA)

So müssen die Anbieter gem. § 4 DiGaV eine Einwilligung des Versicherten für die Verarbeitung der Gesundheitsdaten gem. Art. 9 Abs. 2 lit. a DSGVO einholen.

Diese Einwilligung ist streng zweckgebunden und darf nur zu folgenden Zwecken eingeholt werden:

- Nr. 1.: Zu dem **bestimmungsgemäßen Gebrauch** der digitalen Gesundheitsanwendung durch die Nutzer
- Nr. 2.: Zu dem **Nachweis positiver Versorgungseffekte** im Rahmen einer Erprobung nach § 139e Absatz 4 des Fünften Buches Sozialgesetzbuch
- Nr. 3.: Zu der **Nachweisführung bei Vereinbarungen** nach § 134 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch

Beabsichtigt der DiGA-Anbieter eine Verarbeitung zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung nach § 4 Abs. 2 Nr. 4 DiGaV, so darf er dies nur aufgrund einer zusätzlichen Einwilligung.



Datenverarbeitung außerhalb Deutschlands

Privacy Shield, kein US-Transfer und auch keine US-Anbieter mit EU Servern, neue SSCs, Einwilligungen nach Artikel 49

Die DiGAV erlaubt eine Datenverarbeitung in

der Bundesrepublik Deutschland

Mitgliedstaaten der EU

Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum

Staaten mit Angemessenheitsbeschluss nach Art. 45 DSGVO

Eine Verarbeitung von personenbezogenen Daten außerhalb der EU auf Basis von Art. 46 DSGVO (Standardvertragsklauseln) oder Art. 47 (Corporate Binding Rules) **ist für DiGA nicht zulässig.**

Anforderungen an die Datensicherheit: Sicherheit als Prozess

Bis 2022 wird von DiGA-Herstellern noch keine Umsetzung eines ISMS gemäß ISO-2700-Reihe oder BSI-Standard 200-2 gefordert

Dennoch verlangt die DiGAV in Anlage 1 für alle DiGA das Aufsetzen und Etablieren einer Reihe von Prozessen, um den Grundgedanken von **Sicherheit als Prozess** beim Hersteller zu verankern und die Fortschreibung eines einmal erreichten Sicherheitsniveaus abzusichern:

- Schutzbedarfsanalyse
- Release-, Change- und Configuration-Management:
- Verzeichnis von genutzten Bibliotheken und Marktbeobachtung

ISO27001 → Internationaler Standard für die Informationssicherheit

ISO13485 → Qualitätsmanagementsystem für Medizinprodukte

Datenschutz leicht gemacht mit der Pridatect Plattform

Risiken rechtzeitig erkennen

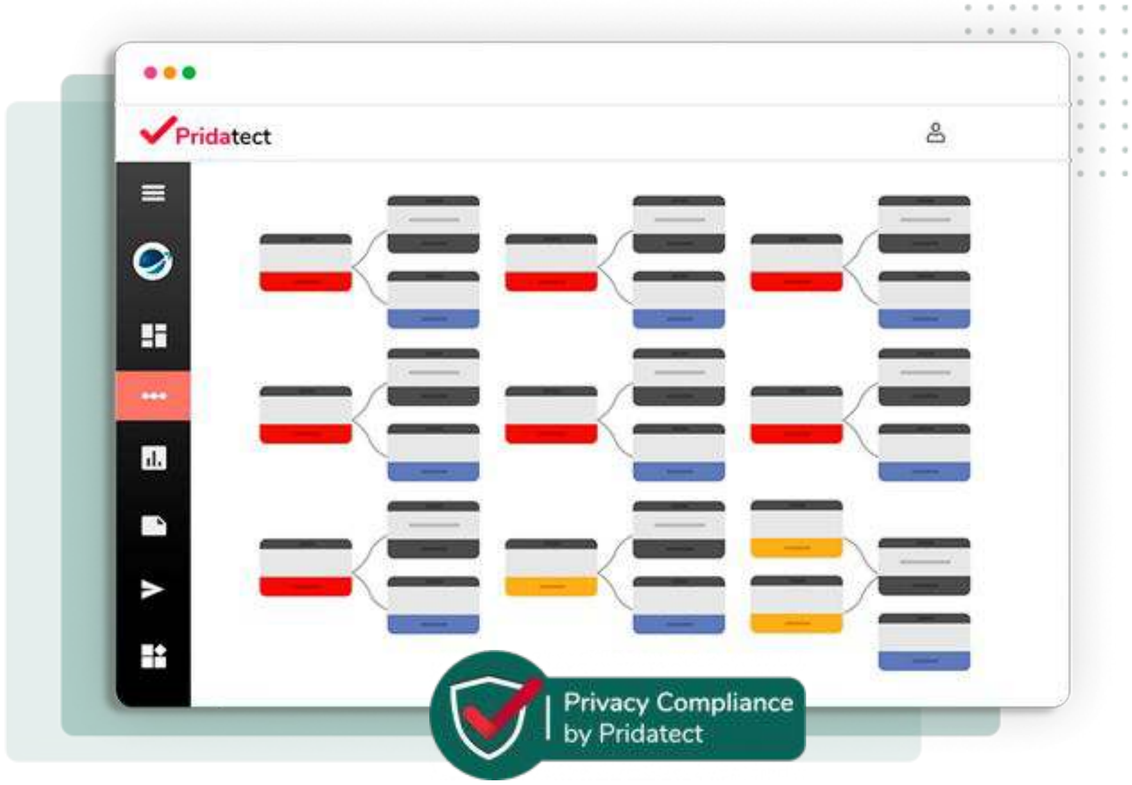
Erkennen und identifizieren Sie Risiken bei der Verarbeitung personenbezogener Daten (Kunden, Mitarbeiter, Anbieter ...). Mit der Pridatect-Plattform können Bedrohungen und Schwachstellen in Ihren Prozessen leicht identifizieren und analysiert werden.

Datenschutzmaßnahmen implementieren

Pridatect meldet notwendige Maßnahmen und erstellt Aufgaben für die in ihrem Unternehmen zuständigen Abteilungen zur Risikoreduzierung. So wird die Umsetzung des Datenschutzes in ihrem Unternehmen leicht gemacht.

Ständige Überwachung und Benachrichtigungen

Datenschutz ist eine ständige Aufgabe innerhalb eines Unternehmens. Pridatect hilft nicht nur bei der ersten Implementierung, sondern auch bei der laufenden Überwachung und Alerts weisen auf notwendige Änderungen, Aktualisierungen und Aufgaben hin.



Bewährte Technologie für Ihren Datenschutz

Alles, was Sie für ein erfolgreiches Datenschutzprogramm benötigen

Risikobewertung

Reduzieren Sie Ihre Datenschutzrisiken

Folgenabschätzungen

Automatisierte Datenschutz-Folgenabschätzungen

Datenschutz-Compliance-Analyse

Identifizieren Sie Lücken in Ihrem Datenschutz

Verarbeitungstätigkeiten

Ein aktualisiertes Verzeichnis Ihrer Verarbeitungstätigkeiten

Datenkarte

Alle Datenflüsse Ihres Unternehmens visuell abgebildet

TOMs

Definieren Sie risikomindernde technische und organisatorische Maßnahmen

Datenschutzberichte

Generieren Sie automatisch notwendige Datenschutzberichte

Internationale Datenflüsse

Verwalten Sie internationale Datenübertragungen

Datenpannen Verwaltung

Reagieren Sie DSGVO-konform auf Datenpannen

Webseiten-Compliance

Generieren Sie Impressum, Datenschutzerklärung und Cookie-Richtlinien

Verbraucheranfragen

Reagieren Sie richtig auf Verbraucheranfragen

Aufgabenmanagement

Teamarbeit in unserer sicheren Cloud-Umgebung

Externer DSB Service

Wir sind ihr externer Datenschutzbeauftragter

AV Verträge

Generieren Sie DSGVO-konforme AV-Verträge

Dokument-Automatisierung

Erstellen Sie Rechtsdokumente basierend auf unseren Modellen

Spezifische Dienstleistungen für Unternehmen im Gesundheitssektor

Bestellung eines Datenschutzbeauftragten (DSB)
Jedes Unternehmen im Gesundheitssektor muss einen Datenschutzbeauftragten ernennen. Pridatect bietet die Bestellung eines externen DSBs an.

Verzeichnis der Verarbeitungstätigkeiten Durch ein virtuelles Data-Mapping werden alle Datenflüsse im Unternehmen ermittelt und dienen als Grundbaustein des Datenschutzprogrammes

Datenschutz-Folgenabschätzungen Beim Umgang mit sensiblen Daten ist die Durchführung von Folgenabschätzungen obligatorisch. Pridatect erleichtert die Implementierung dieser für jede der vom Unternehmen durchgeführten Verarbeitungstätigkeiten.

Gerade als Unternehmen im Bereich Digital Health sind die Augen bzgl. Datenschutz sehr stark auf einen gerichtet. Bei Pridatect hat uns - neben der Plattform - insbesondere das persönliche Gespräch überzeugt. Die Möglichkeit ohne monatliche Zusatzkosten kurze Anliegen schnell zu klären ist sehr wertvoll, da damit wichtige Fragen auch angesprochen und nicht aus falschem Kostenbewusstsein zurückgestellt werden.

mentalis

Hans-Jürgen Stein
Co-Founder and COO mentalis
App für psychische Gesundheit, aktuell im DiGA-Prozess

Probieren Sie es einfach selber aus!

Finden Sie heraus wie Pridatect Ihnen mit Ihrem Datenschutz helfen kann

Übernehmen Sie die Kontrolle über das Datenschutzmanagement und stellen Sie sicher, dass alle Mitarbeiter in Ihrem Unternehmen über die erforderlichen Richtlinien verfügen, um personenbezogene Daten beim Arbeiten im Home Office nicht zu gefährden. Wir von Pridatect helfen Ihnen, Risiken zu erkennen und geeignete Maßnahmen zu ergreifen.

Kostenlose Demo buchen

Kontaktieren Sie uns für eine kostenlose Demo oder nutzen Sie unsere 7-Tage-Testversion.

Lisa Hofmann

Chief of Legal Operations
Pridatect

TÜV zertifizierte
Datenschutzbeauftragte

LinkedIn

Natalya Spuling

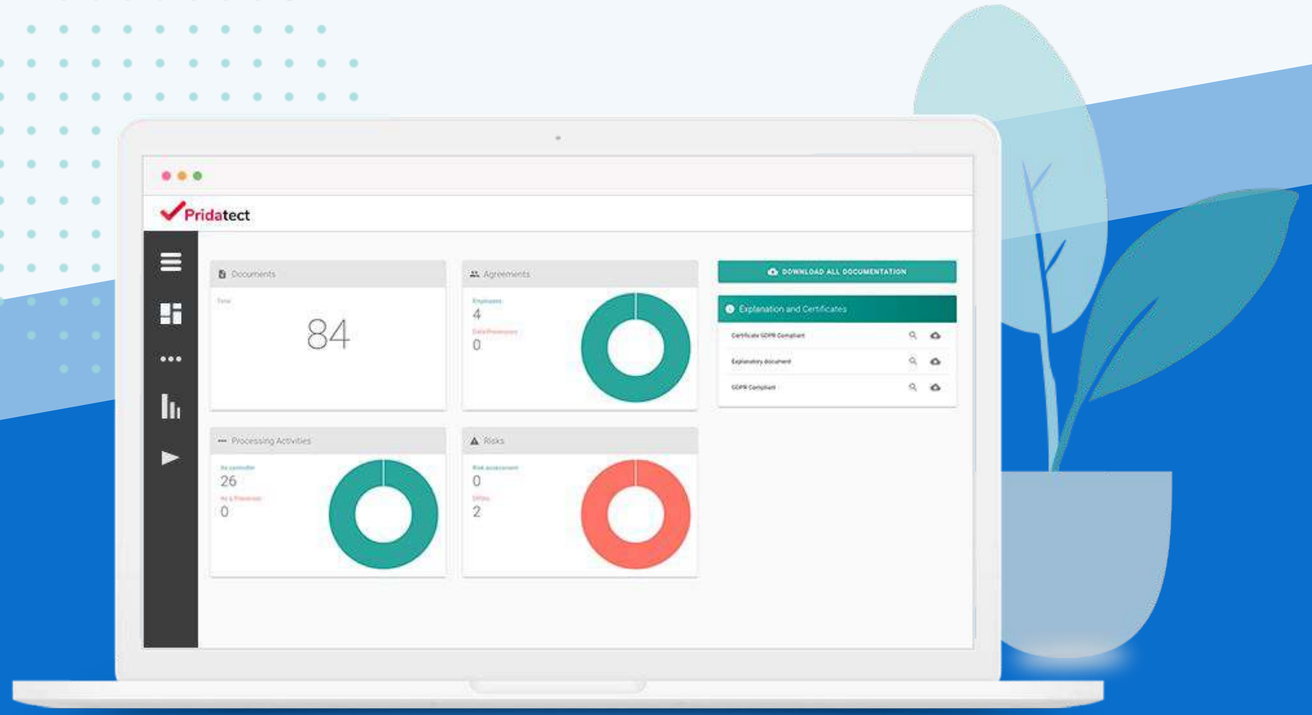
Rechtsanwältin und
Datenschutzbeauftragte

Gesundheitsdatenschutz,
Skill Mentor GDPR
#EUvsVirus

LinkedIn

Senden Sie uns Ihre Fragen

lisa.hofmann@pridatect.com



Vielen Dank, für Ihre Teilnahme an unserem Webinar!

ISO 13485 - Qualitätsmanagementsystem für das Design und die Herstellung von Medizinprodukten

- Norm, die die Erfordernisse für ein umfassendes **Qualitätsmanagementsystem für das Design und die Herstellung von Medizinprodukten** repräsentiert
- Anforderungen an Hersteller und Anbieter von Medizinprodukten bei Entwicklung, Umsetzung und Aufrechterhalten von Qualitätsmanagementsystemen
- Die aktuelle Ausgabe ist **2016 veröffentlicht** worden und ersetzt direkt die letzte Version aus dem Jahr 2012.

Kernanspruch der ISO 13485: **Produktsicherheit und -wirksamkeit.**

ISO 27001 - Zertifizierung auf Basis von IT-Grundschutz

Norm für **Informationssicherheit** in privaten, öffentlichen oder gemeinnützigen Organisationen

- Anforderungen für das **Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheits-Managementsystems (ISMS) von Unternehmen, öffentlichen oder gemeinnützigen Organisationen**

- **Ein ISMS etabliert Prozesse und Richtlinien, mit denen Informationen (und damit auch personenbezogene Daten) verwaltet und geschützt werden sollen.**

- **Aufgaben:**
  - **Prozesse und Richtlinien für Datenverarbeitung im Unternehmen aufstellen**
  - **Informationssicherheit / Datenschutz regeln, steuern, dokumentieren und kontrollieren**
  - **Technische und organisatorische Maßnahmen (TOM) realisieren**
  - **Sicherheitsrisiken aufdecken und reduzieren**

Nach Art. 32 DSGVO sind Unternehmen bereits verpflichtet, ein **Managementsystem für die Verarbeitung von personenbezogenen Daten zu etablieren**. Zur Effizienzsteigerung ist es dabei sinnvoll, ein Managementsystem für alle Informationen – egal, ob personenbezogen oder nicht, digital oder in Papierform – einzuführen. Für ein solches ISMS definiert die ISO 27001 rund **150 Anforderungen und Maßnahmen**, die allerdings je nach Art des Unternehmens oder der Organisation individuell angepasst werden können.