Ausgabe 01 | 2021

SONDERAUSGABE

ExperSite
Digitalisierung, Informationssicherheit und Datenschutz

Das Krankenhauszukunftsgesetz und Informationssicherheit

Mit ganzheitlichen Projektansätzen zum Erfolg

INHALT

EDITORIAL

Wer jetzt nicht strukturiert aktiv wird, verpasst den Anschluss!

Und diesmal geht es um viel Geld. Das Krankenhauszukunftsgesetz bringt für viele Krankenhäuser eine langersehnte Chance, um auf den Digitalisierungszug aufzuspringen, bisher versäumte oder nicht im Budget abgedeckte Leistungen abrufen zu können. Wer sich hier nicht mit einer ganzheitlichen Planung auseinandersetzt, der verpasst die die Chance von erheblichen Fördersummen. Ein bisher auf vielen Ebenen völlig unterschätztes und teilweise auch falsch verstandenes Thema ist die Förderfähigkeit von Informationssicherheit.
Das Krankenhauszukunftsgesetz stellt besonders Maßnahmen für die Informationssicherheit in den Vordergrund, um die Funktionsfähigkeit der medizinischen Einrichtung und die Sicherheit der dort verarbeiteten Patienteninformationen auch zukünftig zu gewährleisten.
Ganz wichtig: wir sprechen hier von Informationssicherheit und nicht etwa von IT-Sicherheit. Das Krankenhauszukunftsgesetz stellt besonders Maßnahmen für die Informationssicherheit in den Vordergrund, um die Funktionsfähigkeit der medizinischen Einrichtung und die Sicherheit der dort verarbeiteten Patienteninformationen auch zukünftig zu gewährleisten. Ganz wichtig: wir sprechen hier von Informationssicherheit und nicht etwa von IT-Sicherheit.
Warum eine Unterscheidung hier von elementarer Bedeutung ist und wie Sie Ihrer Verpflichtung nachkommen, ausreichend Informationssicherheit zu erbringen, ist Kernaspekt dieser Sonderausgabe, damit Sie bis 2025 die entsprechenden Maßnahmen umsetzen können.

Wir räumen in dieser Ausgabe von Grund auf mit Begrifflichkeiten auf, erläutern Ihnen die wichtigsten Fakten rund um das Krankenhauszukunftsgesetz und zeigen Ihnen an Beispielen auf, welche Arten von Informationssicherheit fördern lassen können.

Neben diesem Whitepaper finden zudem regelmäßige Roundtable und Informationsveranstaltungen zu diesem Thema statt, indem wir Ihnen beratend zur Seite stehen.

Wir wünschen Ihnen viel Freude bei der Lektüre

Ihre Nina Richard

DAS WICHTIGSTE IN KÜRZE

Mit dem Krankenhauszukunftsgesetz (KHZG) leistet der Bund einen wichtigen finanziellen Beitrag für die digitale Zukunftsfähigkeit der Krankenhausinfrastruktur. Insgesamt werden in den nächsten Jahren über 4 Milliarden Euro Fördermittel für Krankenhäuser von Bund und Ländern zur Verfügung gestellt.

Investitionen in die Informationssicherheit richtig fördern lassen

Die strategische und konzeptionelle Herangehensweise an das Thema Informationssicherheit ist hier grundlegender Bestandteil, der mit mindestens 15% in allen Förderprojekten berücksichtigt werden muss. Für kleinere Krankenhäuser lohnt sich die Förderung fast doppelt, denn Nicht-KRITIS-Krankenhäuser sind ab dem 1. Januar 2022 verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind (§75c SGB V).

Damit soll das Sicherheitslevel der Telematik-Infrastruktur der deutschen Krankenhäuser angehoben und an den Stand der Technik angeglichen werden. Gleichzeitig sind damit auch Krankenhäuser, die bislang nicht unter die KRITIS-Definition gefallen sind, aufgefordert, bis Ende 2021 ein Management für Informationssicherheit nachzuweisen. Der Förderzeitraum dafür endet am 31.12.2021. Ab 2025 werden bei allen Krankenhäusern zahlreiche geförderte Projektfelder vom Gesetzgeber vorausgesetzt. Krankenhäuser, die sich weigern, werden hier vom Gesetzgeber zur Kasse gebeten.

Informationssicherheit in zwei Paketen

Informationssicherheit wird demnach

1. begleitend für jedes Digitalisierungsprojekt im Sinne
   von privacy- und security-by-design verpflichtend und mit mindestens 15% gefördert.
2. förderfähig im Rahmen des Fördertatbestandes 10
3. für Nicht-Kritis Einrichtungen verpflichtend, um ein ISMS,
   mit all seinen begleitenden Maßnahmen, zu implementieren.

Die DATATREE AG unterstützt, gemeinsam mit Ihren Partnern der Dr. Jäschke AG sowie der Digital Avantgarde GmbH im Rahmen des Krankenhauszukunftsgesetzes. Von der Antragsstellung, Projektierung Ihrer Digitalisierungsprojekte, über den Aufbau eines Informationssicherheitsmanagementsystems, bis hin zur Umsetzung einzelner Maßnahmen, begleiten unsere Experten Sie.

1. DAS KRANKENHAUSZUKUNFTSGESETZ

1. DAS KRANKENHAUSZUKUNFTSGESETZ

„Das Krankenhauszukunftsgesetz (KHZG) ist, richtig angewendet, eine der größten Chancen, sich als Krankenhaus mit einer gezielten Digitalisierungsoffensive zukunftsfähig aufzustellen." (Digital Avantgarde GmbH). Gleichzeitig bringt es allerdings auch vielzählige Pflichten mit sich: Wer sich der Digitalisierung gegenüber verschließt, der zahlt. In der Umsetzung bedeutet dies, dass Kliniken, die keine Digitalisierungsprozesse auf Basis der Telematikinfrastruktur nachweisen können, ab dem Jahr 2025, basierend auf allen voll- und teilstationären Fällen, einen Abschlag von bis zu zwei Prozent zahlen müssen.

Die Ziele des Krankenhauszukunftsfond liegen auf der Hand. Neben der Steigerung der Versorgungsqualität soll auch die Nutzung der Anwendungen der Telematikinfrastruktur gefördert werden, um TI-Applikationen im Alltag der Ärzte, Apotheker und Patienten mit zu etablieren. Nur so können sich Kliniken effizienter, stark und für Ihre Zielgruppe bedarfsgerecht aufstellen, um für die Zukunft gewappnet zu sein.

Durch das KHZG sollen folgende Bereiche gefördert werden:

- moderne Notfallkapazitäten,
- patientenzentrierte Mehrwertdienste,
- Ablauforganisation,
- Kommunikation,
- Telemedizin,
- die gezielte Stärkung regionaler Versorgungsstrukturen.

Eines der Schlüsselziele ist die Vernetzung, um so den Insellösungen den Rücken zu kehren. Ein besonders großer Stellenwert kommt hier dem Bereich der Informationssicherheit zu. Demnach müssen mindestens 15% der Fördergelder je Maßnahme in den Bereich der Informationssicherheit fließen. Des Weiteren fordert das BMG Kliniken auf, sich schon frühzeitig mit den Fördermöglichkeiten auseinanderzusetzen, damit Digitalprojekte zügig angegangen werden können.

Nach dem KHZG geförderte Digitalisierungsprojekte müssen mindestens 15 % des Fördervolumens für Maßnahmen der Informationssicherheit verwenden. Die erfahrenen Experten für Informationssicherheit und Datenschutz der DATATREE AG unterstützen Sie für den Erfolg Ihres Digitalisierungsprojektes.

Ganzheitliche Projektierungen von Digitalisierungsvorhaben müssen frühzeitig gedacht und innerhalb der Förderanträge berücksichtigt werden. So fallen auch Projekte unter die Richtlinie und können gefördert werden, wenn diese bereits seit 02. September 2020 begonnen oder durchgeführt wurden. Die Umsetzung der Förderung selbst erfolgt über die Länder. Anträge können bis Ende 2021 beim Bundesamt für soziale Sicherung (BAS) gestellt werden.

1.1 DIE EINORDNUNG VON PATIENTENDATENSCHUTZGESETZ, SGB V. UND KHZG

Das PDSG bringt als „Omnisbus"- oder „Containergesetz" weitreichende Änderungen für viele andere Gesetze. So werden unter anderem Artikel 1 des PDSG diverse Änderungen im SGB V verfügt. So wird der § 75 b dahingehend geändert, dass nun mehr auch alle niedergelassenen Ärzte, die an der vertragsärztlichen Versorgung teilnehmen, Maßnahmen zur Informationssicherheit umsetzen müssen. Weiter wird § 75 c SGB V eingefügt, der nunmehr festlegt, dass alle Krankenhäuser bis zum 01.01.2022 die Anforderungen des § 8a BSIG umsetzen müssen, auch wenn sie nicht zur kritischen Infrastruktur gehören.

Danach sind alle Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind(§ 75 c SGB V). Die Anforderungen dafür bildet der vom BSI anerkannte B3S (Branchen-spezifischer Sicherheitsstandard) für die medizinische Versorgung.

Da bei allen nach dem KHZG geförderten Digitalisierungsprojekten mindestens 15 % des Fördervolumens für Maßnahmen der Informationssicherheit zu verwenden sind, können die gesetzlichen Anforderungen aus § 75 c SGB V mit Mitteln des KHZG gefördert werden. Dies gilt nur für Nicht-KRITIS Häuser, da diese für die Umsetzung der KRITIS-Anforderungen den Krankenhausstrukturfond 2.0 nutzen können. Die Verbesserung der IT-Sicherheit hat der Bund 2019 als neuen Fördertatbestand in den Krankenhausstrukturfonds aufgenommen. Für die aktuelle Förderperiode 2019-2024 stehen beim Amt für Soziale Sicherung nun nicht mehr 500 Millionen, wie in der ersten Förderperiode, sondern insgesamt 750 Millionen Euro zur Verfügung.

1.2 ZAHLEN UND FAKTEN

Folgend die wichtigsten Zahlen und Fakten zum Krankenhauszukunftsgesetz im Überblick:

- Krankenhauszukunftsfonds = 3 Mrd € (Bund)
- Kofinanzierung durch das jeweilige Land oder Träger in Höhe von bis zu 1,3 Mrd €
- Die meisten Bundesländer haben die Co-Finanzierung der Bundesförderung fest eingeplant
- Maximal 10% der Mittel für Vorhaben an Hochschulkliniken
- Digitalisierungsvorhaben Nr. 2-6 geknüpft an Voraussetzungen (Interoperabilität ePA usw.)
- Mind. 15% des Vorhabens für IT-Sicherheit/Informationssicherheit
- Antragsfrist für die Länder bis 31. Dezember 2021

Die untenstehende Tabelle gibt eine Übersicht über die Verteilung der 4,3 Milliarden EURO nach dem Königsteiner Schlüssel (KSS). Die letzten beiden Spalten dienen der groben Orientierung, mit welcher Fördersumme ein Krankenhaus pro Bett bei einer theoretischen „Gießkannenverteilung“ rechnen kann. Diese kann nach beliebigen anderen Faktoren berechnet werden und dient lediglich einer Orientierung (vgl. Digital Avantgarde).

1.3 TERMINE UND DEADLINES IM ÜBERBLICK

Um erfolgreich Fördermittel zu beantragen, sind einige Deadlines im Blick zu halten.

seit dem 02.09.2020
Auch bereits begonne Projekte sind förderfähig!

31.12.2020
Gesetzlich festgelegter Termin: Anbindung an die Telematikinfrastruktur muss bereits vollzogen sein

in Vorbereitung auf

01.01.2021
Einführung der elektronischen Patientenakte (ePA)

31.12.2021
Frist für die Einreichung der Anträge auf die Förderung nach dem KHZG beim BAS

01.01.2022
Maßnahmen nach dem B3S im Rahmen des §75c SGB V sind umzusetzen und alle 2 Jahre anzupassen

2025
Krankenhäuser müssen zahlen, wenn sie ihre Prozesse nicht digitalisiert haben!

→ Bis zu zwei Prozent Abschlag auf die Abrechnung aller voll- und teilstationären Fälle

Weitere Informationen zu Terminen und Deadlines →

Alle Projekte, die **seit dem 02.09.2020** bestehen sind förderfähig, sodass auch bereits begonnene Projekte förderfähig sind. Krankenhäuser müssen bis zum gesetzlich festgelegten Termin am **31.12.2020** die Anbindung an die Telematikinfrastruktur vollzogen haben, um auf die Einführung der elektronischen Patientenakte (ePA) zum **01.01.2021** vorbereitet zu sein. Anträge auf die Förderung nach dem KHZG müssen bis zum **31.12.2021** beim BAS eingegangen sein. Kliniken, die von den Digitalisierungs-Milliarden profitieren wollen, müssen den praktischen Einsatz der TI-Anwendungen nachweisen. Die Mittel aus dem Fördertopf werden vergeben, bis sie aufgezehrt sind. Maßnahmen nach dem B3S im Rahmen des § 75c SGB V sind bis zum **01.01.2022** umzusetzen und anschließend **alle 2 Jahre** anzupassen.

Krankenhäuser, die **bis 2025** ihre Prozesse nicht digitalisiert haben, erhalten nicht nur keine Fördermittel, sondern müssen zahlen. Der Malus beträgt bis zu zwei Prozent Abschlag auf die Abrechnung aller voll- und teilstationären Fälle ab 2025. Bereits mit dem Verpassen der Frist für die technische Anbindung an die Telematikinfrastruktur zum **31.12.2020** ist ein solcher Abschlag verbunden. Im Digitale-Versorgung-Gesetz heißt es zu der TI-Frist: „Die Krankenhäuser haben sich bis zum **1. Januar 2021** mit den für den Zugriff auf die elektronische Patientenakte erforderlichen Komponenten und Diensten auszustatten und sich an die Telematikinfrastruktur nach § 291a Absatz 7 Satz 1 anzuschließen. Soweit Krankenhäuser ihrer Verpflichtung zum Anschluss an die Telematikinfrastruktur nach Satz 4 nicht nachkommen, ist § 5 Absatz 3e Satz 1 des Krankenhausentgeltgesetzes oder § 5 Absatz 5 der Bundespflegesatzverordnung anzuwenden."

Der entsprechende Paragraf des Krankenhausentgeltgesetzes (KHG) sieht vor, dass „für die Zeit ab dem **1. Januar 2022** ein Abschlag in Höhe von einem Prozent des Rechnungsbetrags für jeden voll- und teilstationären Fall, sofern ein Krankenhaus seiner Verpflichtung zum Anschluss an die Telematikinfrastruktur nach § 291 Absatz 2c Satz 4 des Fünften Buches Sozialgesetzbuch nicht nachkommt" zwischen dem GKV-Spitzenverband und der DGK umgesetzt werden soll.

Der Krankenhauszukunftsfonds ist also eigentlich ein Krankenhausdigitalisierungsfonds, der die Nutzung der Anwendungen der Telematikinfrastruktur verbindlich vorschreibt und den Einsatz der TI-Applikationen im Alltag der Ärzte, Apotheker und Patienten etablieren soll.

ZEITPLAN NACH KRANKENHAUSZUNKUNFTSGESETZ

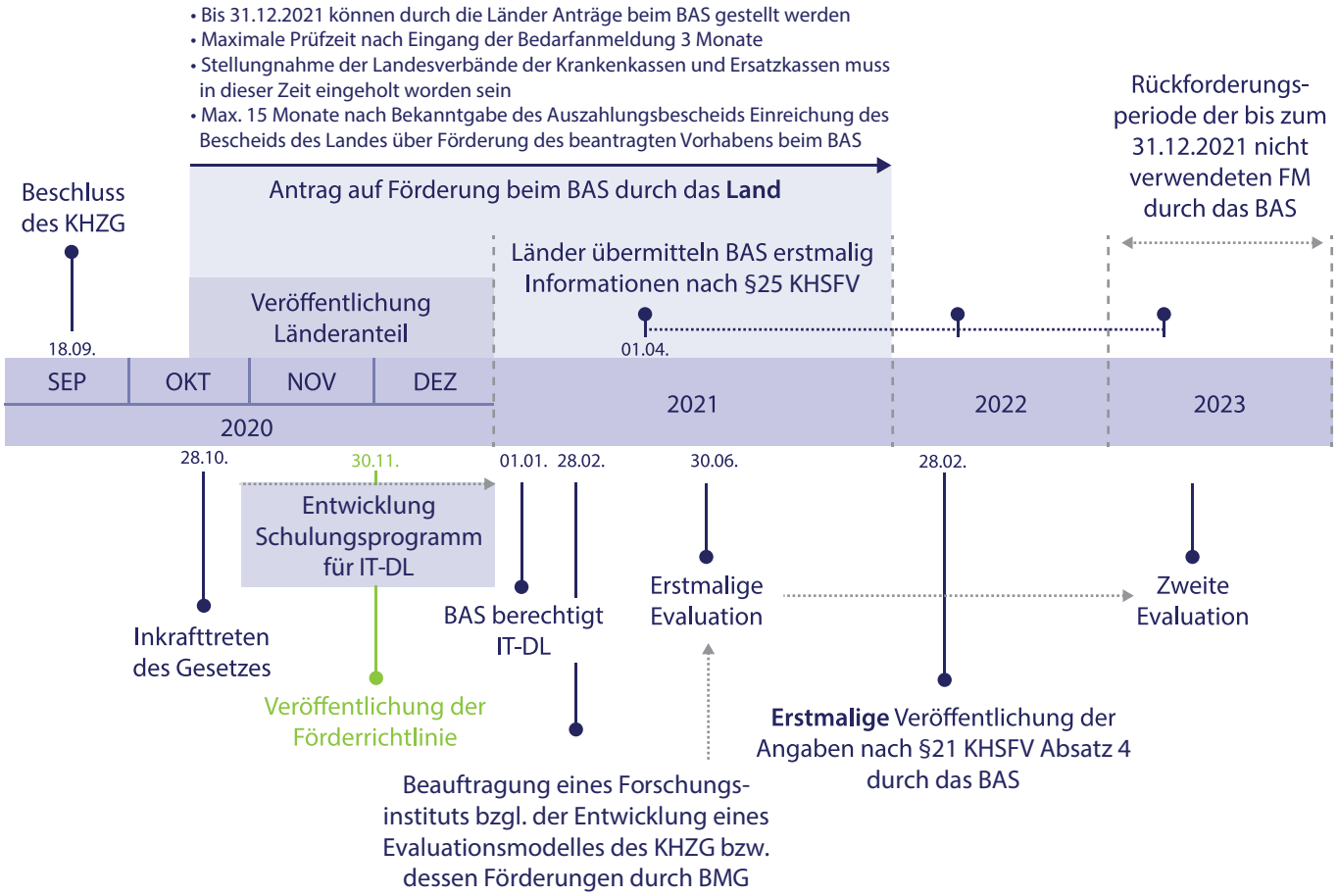


Abbildung in Anlehnung an die Grafik des Bundesamtes für Gesundheit

https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/K/Krankenhauszukunftsfonds_Zeitplanung.png

2. INFORMATIONSSICHERHEIT, DATENSCHUTZ UND IT-SICHERHEIT

2. INFORMATIONSSICHERHEIT, DATENSCHUTZ UND IT-SICHERHEIT

Den Begriffen Informationssicherheit, Datenschutz und IT-Sicherheit kommt eine besondere Bedeutung zu. Bereits im „Gesetz für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz – KHZG)" mit Bundestagsbeschluss vom 23. Oktober 2020 wird die Notwendigkeit, Anforderungen an die Informationssicherheit zu erfüllen, in den Vordergrund gestellt. Daher sind mindestens 15 Prozent der gewährten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden.

In der Folge wurde entsprechend der Fördertatbestand 10, konkret die Förderung der IT-Sicherheit nach KHSVF §19 Abs. 1 Satz 1 Nr. 10 in die Förderrichtlinie aufgenommen:

> *„...die Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer oder kommunikationstechnischer Anlagen, Systeme oder Verfahren, um die nach dem Stand der Technik angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Krankenhausträgers zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind, ..."*

Die Vorhaben sind nach Vorgaben des § 19 Abs. 2 KHSFV nur förderfähig, wenn, unter anderem:

- **Maßnahmen zur Gewährleistung der Informationssicherheit nach dem jeweiligen Stand der Technik durchgehend berücksichtigt werden, und**
- **datenschutzrechtliche Vorschriften eingehalten werden.**

Die Begriffe Datenschutz, Datensicherheit, Informationssicherheit und IT-Sicherheit sowie Cyber Security werden jedoch nicht erst im Zuge des KHZG häufig in einer Art und Weise synonym verwendet, die nicht förderlich ist. Tatsächlich adressieren die Begriffe Datensicherheit und Informationssicherheit die gleichen Inhalte. Etabliert hat sich jedoch der Begriff der Informationssicherheit. Hintergrund ist, dass der Wert von einzelnen Daten steigt, wenn diese in einen Zusammenhang gebracht werden. Diesen entstandenen Mehrwert gilt es zu schützen, was durch die Verwendung des Begriffs der Informationssicherheit deutlich wird.
Wie alle Anforderungen an die Compliance liegt Informationssicherheit in der Verantwortung der Geschäftsleitung und ist damit ein zentrales Thema des Managements.

Besondere Informationen sind personenbezogene Daten, denen wegen ihres Schutzbedarfs ein spezielles Gesetz gewidmet ist: die EU-DSGVO (Europäische Datenschutzgrundverordnung) bzw. das BDSG (Bundesdatenschutzgesetz). Gesprochen wird hier, wie hinlänglich bekannt, vom Datenschutz. Sowohl in der Informationssicherheit als auch im Datenschutz geht es nicht ausschließlich um elektronisch verarbeitete Daten, wenngleich der Großteil der Informationen aller Art in IT-Systemen verarbeitet wird.

Die IT-Sicherheit leitet sich dagegen aus der Informationssicherheit ab und schützt durch technische und organisatorische Maßnahmen die schützenswerten Informationen. Der Begriff Cyber Security zielt ebenfalls darauf ab, umfasst aber noch mehr die Sicherheit auch im Sinne der Gefahren aus dem Internet.

Eine Firewall allein erhöht nicht die Informationssicherheit. Notwendig ist eine strategische Berücksichtigung der Informationssicherheit in der Digitalen Transformation, aus der sich dann Maßnahmen zur Erhöhung der IT-Sicherheit ableiten. Dies kann dann auch eine Firewall sein oder ein Intrusion Prevention System.

Datenschutz ≠ **Informationssicherheit**

- Schutzbedarf personenbezogener Daten
- Gesetzliche Grundlage: EU-DSGVO und BDSG

- zentrales Thema des Managements
- Schutz aller Informationen und Assets eines Unternehmens

IT-Sicherheit → **Cyber Secuirty**

- Schützt durch technische und organisatorische Maßnahmen die schützenswerten Informationen
- Sicherheit im Sinne der Gefahren im Internet

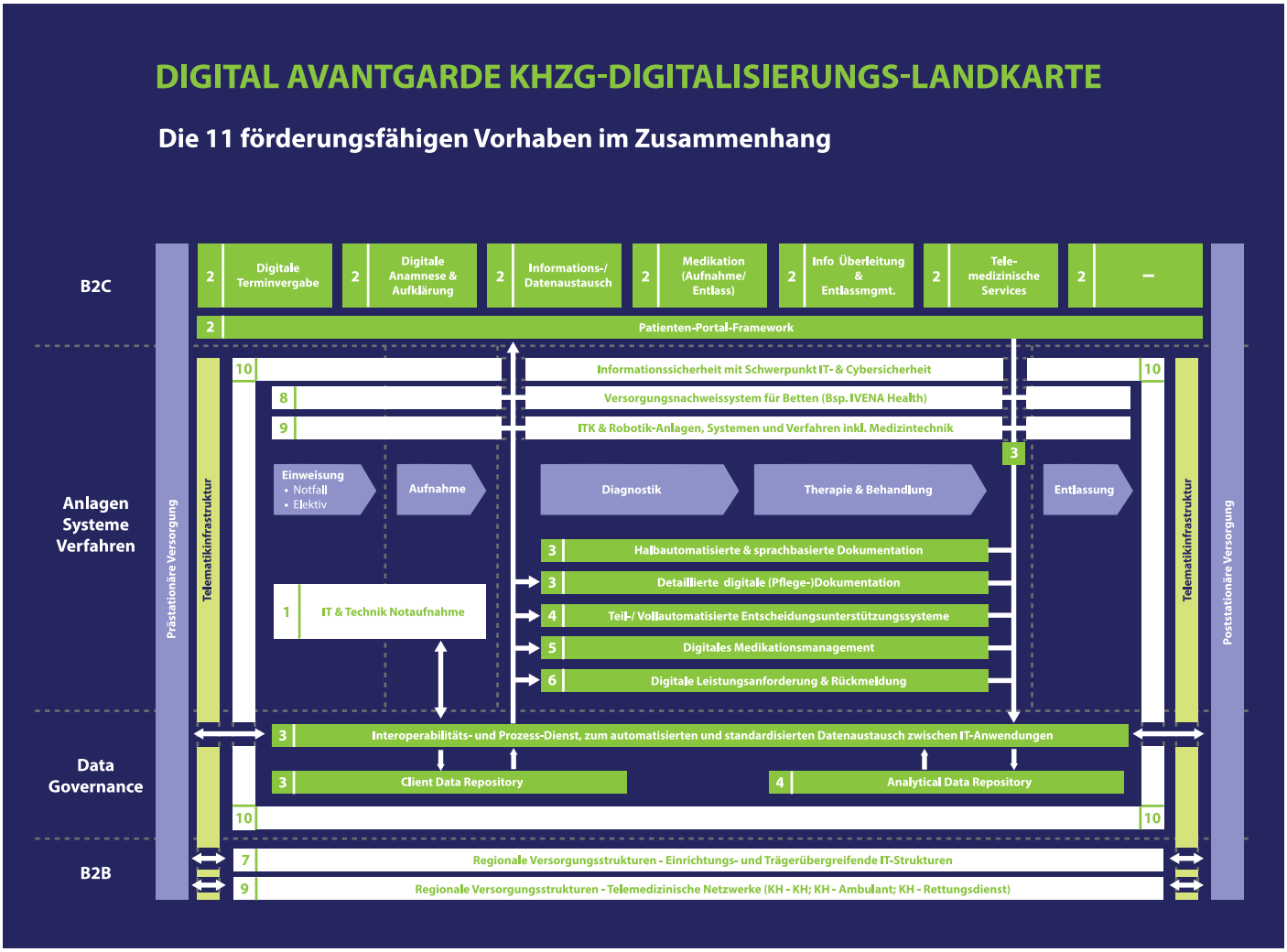
3. FÖRDERFÄHIGE VORHABEN

3. FÖRDERFÄHIGE VORHABEN

Zur Identifikation von förderfähigen Vorhaben hat die DATATREE AG und deren verbundene Unternehmen eine hohe, nachgewiesene Fachexpertise, mit der wir Sie auf dem kompletten Weg der Digitalisierung umfänglich begleiten werden.

3.1 PROJEKTIERUNG: DIGITALISIERUNGS-LANDKARTE DER DIGITAL AVANTGARDE §19

Die Digital Avantgarde GmbH betreut Krankenhäuser und Kliniken bei der ganzheitlichen Betrachtung und Projektierung von Digitalisierungsvorhaben. Vom Digitalisierungs-Workshop, über die Antragsstellung, hin zur kontinuierlichen Betreuung innerhalb des Fördervorhabens.



3.2 INFORMATIONSSICHERHEIT - FÖRDERTATBESTAND 10: IT-SICHERHEIT (§19 ABS. 1 SATZ 1 NR. 10 KHSFV)

Neben den bereits erwähnten förderfähigen Anteilen innerhalb eines jeden Digitalisierungsvorhabens, wird dem Aspekt der Informationssicherheit ein weiterer eigener Fördertatbestand hinzugefügt. Ziel des Fördertatbestandes 10 ist die Verbesserung der IT-bzw. Cybersicherheit in Krankenhäusern, die nicht zu den kritischen Infrastrukturen gehören sowie in Hochschulkliniken. Maßnahmen zur Verbesserung der Informations- bzw. Cybersicherheit sind bei diesen Krankenhäusern bisher von der Förderung nach dem Krankenhausstrukturfonds ausgeschlossen.

Auch in Krankenhäusern, die nicht zur kritischen Infrastruktur gehören, führt der zunehmende Grad der Digitalisierung zu steigenden Anforderungen bei der Informations- bzw. Cybersicherheit, der eine Berücksichtigung im Rahmen des Fördertatbestandes Nummer 10 dringend anzeigt.

Um eine optimale Versorgung der Patientinnen und Patienten zu gewährleisten und den Krankenhausbetrieb so effizient wie möglich zu gestalten, ist der Einsatz von zu Teilen hochkomplexen IT-Systemen notwendig und nicht mehr wegzudenken. Durch die zunehmende Vernetzung verschiedener Systeme und Komponenten steigen jedoch auch die Risiken hinsichtlich der Auswirkungen, die mit einem Ausfall oder der Beeinträchtigung ebendieser Systeme verbunden sind, im gleichen Maße. Zeitgleich werden die Angriffsflächen der IT- und Internettechnologien zunehmend vielfältiger und deutlich größer. Diesen muss durch geeignete Maßnahmen entgegengewirkt werden. Hierbei ist sowohl die Sicherheit der IT-Systeme als auch der dabei verarbeiteten Patientendaten in der Gesundheitsversorgung von höchster Bedeutung.

Eine Vermeidung von Störungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse muss sichergestellt sein.

Gleiches gilt für die Authentizität der Daten. Nur so kann die Patientensicherheit und Behandlungseffektivität sowie die Funktionsfähigkeit des Krankenhauses aufrechterhalten und geschützt werden.

Informations- und Cybersicherheit sind die notwendigen Bedingungen für die fortschreitende Digitalisierung in den Kliniken. Dies kann durch ein geeignetes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 oder BSI IT-Grundschutz gesteuert und überwacht sowie insbesondere durch die Umsetzung des Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus vollständig gewährleistet werden.

3.2.1 WEITERE FÖRDERFÄHIGKEITEN IM BEREICH INFORMATIONSSICHERHEIT

Die im Folgenden skizzierten Anforderungen und darin exemplarisch skizzierten Sicherheitssysteme werden nicht solitär innerhalb eines der Bereiche Prävention, Detektion, Mitigation, Response oder Awareness eingesetzt, sodass eine Anwendung mehrere Bereiche abdecken kann.

Funktionale Anforderungen
Förderfähige Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit müssen:

- die Prävention von Informationssicherheits-Vorfällen (u.a. Systeme zur Zonierung von Netzwerken, Next Generation Firewalls, sichere Authentisierungssysteme, Micro-Virtualisierung/Sandbox-Systeme, Schnittstellen-Kontrolle, Intrusion Prevention Systeme; Network Access Control, Schwachstellenscanner, Softwareversionsmanagement, Datenschleusen, Datendioden, VPN-Systeme, verschlüsselte Datenübertragung, verschlüsselte mobile Datenträger, ISMS)

  oder

- die Detektion von Informationssicherheits-Vorfällen (u.a. Security Operation Center, Log Management Systeme, Security Information Event Management Systeme, Intrusion Detection Systeme, lokaler Schadsoftwareschutz mit zentraler Steuerung, Schadsoftwareschutz in Mailsystemen bzw. bei Mailtransport),

  oder

- die Mitigation von Informationssicherheits-Vorfällen (u.a. automatisierte Backup-Systeme, lokaler Schadsoftwareschutz mit zentraler Steuerung)

  oder

- die Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen bzw. der Bedeutung von IT-/Cybersicherheit (u.a. regelmäßige Risikoanalysen, Schulungsmaßnahmen, Informationskampagnen, Awareness-Messungen)

  oder

- eine Kombination davon zum Ziel haben.

Förderfähige Vorhaben zur Verbesserung der Informations- bzw. Cybersicherheit können Cloud- und KI gestützte Verfahren zur Erkennung von Angriffen als Gegenstand haben.

Entwickeln Sie mit der DATATREE-AKADEMIE individualisierte Schulungskonzepte für Ihre Digitalisierungsprojekte und spezifische Awareness-Kampagnen für Ihre Klinik- und Projektmitarbeiter.

4. FÖRDERFÄHIGE KOSTEN

4. FÖRDERFÄHIGE KOSTEN

Bei allen Vorhaben nach §19 Abs. 1 KHSFV können Kosten für technische und informationstechnische Maßnahmen gefördert werden (§20 Abs. 1). Im IT-Bereich fallen daher auch Kosten für Beratung, Softwarelizenzen, Konfigurationskosten und Integrationskosten wie Kosten für Software-as-a-Service / Platform-as-a-Service unter die Fördertatbestände. Diese werden bei den förderungsfähigen Kosten berücksichtigt.

Dazu führt der § 19 Abs. 1 Nr. 10 aus, dass *…die Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer oder kommunikationstechnischer Anlagen, Systeme oder Verfahren, um die nach dem Stand der Technik angemessenen organisatorischen und technischen Vorkehrungen* ***zur Vermeidung von Störungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Krankenhausträgers zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind****, wenn das Vorhaben nicht nach § 12a Absatz 1 Satz 4 Nummer 3 des Krankenhausfinanzierungsgesetzes in Verbindung mit § 11 Absatz 1 Nummer 4 Buchstabe a förderfähig ist, sowie*

Bei den in § 19 Absatz 1 genannten Vorhaben können folgende Kosten erstattet werden:

1. die Kosten für erforderliche technische und informationstechnische Maßnahmen einschließlich der Kosten für Beratungsleistungen bei der Planung des konkreten Vorhabens,
2. die Kosten für erforderliche personelle Maßnahmen einschließlich der Kosten für Schulungen der Mitarbeiterinnen und Mitarbeiter,
3. die Kosten für räumliche Maßnahmen, soweit sie für die technischen, informationstechnischen und personellen Maßnahmen erforderlich sind; bei den in § 19 Absatz 1 Satz 1 Nummer 1 bis 10 genannten Vorhaben dürfen die Kosten für räumliche Maßnahmen jedoch höchstens 10 Prozent der gewährten Fördermittel ausmachen und
4. die Kosten für die Beschaffung von Nachweisen nach § 25 Absatz 1 Nummer 2.

(2) Bei den in § 19 Absatz 1 Satz 1 Nummer 7 genannten Vorhaben können bei erforderlichen technischen und informationstechnischen Maßnahmen insbesondere die Kosten für die Bereitstellung des Systems und für die Anbindung des Krankenhauses oder anderer Leistungserbringer an das System, einschließlich der für die Nutzung erforderlichen Software, erstattet werden. Bei den in § 19 Absatz 1 Satz 1 Nummer 9 und 10 genannten Vorhaben werden bei erforderlichen technischen und informationstechnischen Maßnahmen insbesondere die Kosten des Krankenhauses für die Beschaffung, Errichtung, Erweiterung oder Entwicklung informations- oder kommunikationstechnischer Anlagen erstattet. Die Kosten für die Errichtung nach Satz 2 umfassen auch die unmittelbaren Kosten der Krankenhäuser für die sichere Anbindung an die ambulante Einrichtung.
(3) § 2 Absatz 3 Satz 2 und 3 und Absatz 4 gilt entsprechend.

So wird klar verdeutlicht, dass die Informationssicherheit eine strategische Bedeutung bei der Digitalisierung des Gesundheitswesens darstellt.

4.1 FÖRDERFÄHIGE VORHABEN GEMÄß §19 ABS. 1 KHSFV MIT DER DATATREE AG

Bereits in Vorbereitung auf die Antragsphase gilt es Aspekte der Informationssicherheit vollumfänglich zu berücksichtigen. Die Anforderungsanalyse wird im jeweiligen Fördertatbestand hinsichtlich der Berücksichtigung von Informationssicherheit und Datenschutz durchgeführt.

- Identifizierung der Maßnahmen der Informationssicherheit, IT-Sicherheit und des Datenschutzes
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Identifizierung der notwendigen Infrastrukturmaßnahmen
- Identifizierung des Schulungsbedarfs
- Erstellung von Datenschutzkonzepten
- Erstellung und Erweiterung von IT-Sicherheitskonzepten

4.2 FÖRDERTATBESTAND 10 MIT DER DATATREE AG

Anforderungsanalyse und Abgleich der Anforderungen bezogen auf das KHZG

Maßnahmen der Informationssicherheit:

- Audit zur Informationssicherheit
- Organisation und Verantwortlichkeiten
- Benennung des Informationssicherheitsbeauftragten
- Aufbau und Pflege des ISMS
- Schutzbedarfsanalyse
- Risikoanalyse

Maßnahmen der IT-Sicherheit:

- Audit zur IT-Sicherheit
- Benennung eines IT-Sicherheitsbeauftragten
- Strukturanalyse
- Bedrohungsanalyse
- Ableitung technischer und organisatorischer Maßnahmen
- Erstellung von IT-Sicherheitskonzepten

Maßnahmen zur Steigerung der Awareness und Prüfung der Wirksamkeit:

- Schulungsmaßnahmen
- Informationskampagnen
- Awareness-Messungen
- Social Engineering
- Penetrationstest

5. INFORMATIONSSICHERHEIT RICHTIG ANGEHEN MIT DEM KHZG

Die Grundlage für eine erfolgreiche Projektierung ist die ganzheitliche Betrachtung aller Gegebenheiten und Rahmenbedingungen. Unsere Analyse beginnt mit dem Requierement-Engineering KHZG), woraus sich weiterführende Maßnahmen, wie Datenschutz- oder IT-Sicherheits-Konzepte (ggf. je Fördertatbestand) ableiten. Wir betreuen Sie selbstverständlich kontinuierlich über die komplette Projektlaufzeit.

PHASE	UNSERE PRODUKTE/DIENSTLEISTUNGEN
PHASE 0: VOR DER ANTRAGSSTELLUNG	➡ Requierements-Engineering KHZG (Informationssicherheit)
PHASE 1: DIE ANTRAGSSTELLUNG	➡ Projektbegleitung
PHASE 2: DIE PROJEKTDURCHFÜHRUNG	➡ Risiko-Workshop ➡ Projekt: Aufbau ISMS ➡ IT-Sicherheitsüberprüfung (Security Scan) ➡ Ergebnispräsentation Kontinuierliche Dienstleistungen: ➡ Informationssicherheitsbeauftragter (ISB) ➡ GAIMS
PHASE 3: DAS PROJEKT-CONTROLLING	➡ Informationssicherheits-Audit ➡ Überprüfung der Informationssicherheits-Audits

Unsere Experten der DATATREE AG und Ihrer Schwesterunternehmen begleiten Sie umfangreich von der Antragsstellung bis zur Reifegradevaluierung. Machen Sie das Thema Informationssicherheit zu einem strategischen Thema und sichern sich so die höchstmögliche Fördersumme für Ihre Digitalisierungsprojekte.

PHASE 0 | 1 | 2 | 3

5.1 PHASE 0: VOR DER ANTRAGSSTELLUNG

5.1.1 REQUIEREMENTS-ENGINEERING KHZG (INFORMATIONSSICHERHEIT)

Bereits vor der eigentlichen Antragsstellung ist es notwendig, die Förderprojekte aus Sicht der Informationssicherheit zu betrachten, um die konkreten Antragsinhalte und die Projektbudgetierung vorbereitend für die Antragsstellung vorzunehmen und so die 15% je Fördertatbestand zu erreichen.

Unser gemeinsames Ziel ist die Dokumentation des Soll-Ist-Standes sowie die Identifikation und Bewertung der Projekte mit entsprechenden Maßnahmen.

Part A Compliance-Struktur-Workshop:	Part B Projekt-Workshop:	Part C Abschlussgespräch:
→ Sichtung Organisationsstrukturen, Prozesse und Verantwortlichkeiten → Dienst als Orientierungsworkshop für den Auftraggeber	→ Besprechung und konkrete Projektprüfung → Klärung der Anforderungen von Informationssicherheits- und Datenschutzmanagement → Finalisierung des Soll-Ist-Standes mit dem Bereich IT-Sicherheit und weiterführenden Fachabteilungen	→ Zusammenfassung der Ergebnisse mit konkreten Budgetierungsvorschlägen und Maßnahmenempfehlungen

REQUIEREMENTS-ENGINEERING KHZG (INFORMATIONSSICHERHEIT)
→ **ab 4.458,00 EUR**

Wann ist das Requierements-Engineering KHZG die richtige Wahl?

Sie haben Ihre KHZG-Projekte bereits zu circa 90% umrissen und mit einem Budget belegt.

Sie haben Ihre Projekte noch nicht definiert? Unsere Experten der Digital Avantgarde unterstützen Sie gern. Sprechen Sie uns an.

5.2 PHASE 1: DIE ANTRAGSSTELLUNG

5.1.2 PROJEKTBEGLEITUNG

Der Aufwand zur Koordination von Informationssicherheitsprojekten wird häufig unterschätzt, ebenso, wie die aufkommenden Detailfragen innerhalb der Antragsstellung. Wir lassen Sie nicht im Stich und begleiten Sie, mit unserer Expertise aus vielzähligen Förderprojekten auch innerhalb der Antragsstellung.

Unser gemeinsames Ziel ist die optimale und lückenlose Darstellung der Aspekte der Informationssicherheit(sprojekte) und Projektplanung innerhalb der Antragsphase.

PROJEKTBEGLEITUNG
➡ **ab 1468,00 EUR**

5.3 PHASE 2: DIE PROJEKTDURCHFÜHRUNG

Nachfolgende Leistungen können einzeln oder auch in einem Gesamtmaßnahmenpaket durchgeführt werden.

BESCHREIBUNG

RISIKO-WORKSHOP

Betrachtung der existierenden Verfahren zum Erhalt der Werte und Assets der Organisation anhand von anerkannten Best-Practice Verfahren, wie z.B. der ISO 27001 Norm. Das Ziel ist die Dokumentation des Soll-Ist-Standes, die Identifikation und Bewertung daraus abgeleiteter Risiken sowie die Priorisierung bzw. Empfehlung weiterer Handlungsschritte.

Vorbereitung, Durchführung, Nachbereitung

Die Workshop-Durchführung dauert (abhängig von der Klinikgröße) in der Regel 1-4 Personentag(e).

BESCHREIBUNG

PROJEKT: AUFBAU ISMS

Implementierung eines branchenspezifischen Managementsystems für Informationssicherheit (ISMS) und der Aufbau einer Informationssicherheits-Organisation beim Auftraggeber.

BESCHREIBUNG

IT-SICHERHEITSÜBERPRÜFUNG (SECURITY SCAN)

Durchführung eines Security Scans (Penetrationstest) Ihrer externen (aus dem Internet) oder internen IT-Systeme (z.B. Web-/Mail-/Applikationsserver), um kritische Schwachstellen und mögliche Verwundbarkeiten aufzudecken. Verwendung von automatisierten Scantechniken mit einer manuellen Verifizierung der Scanergebnisse. Dokumentation und Zusammenfassung der Abweichungen in einem Bericht inklusive Benennung von Maßnahmenvorschlägen.

BESCHREIBUNG

ERGEBNISPRÄSENTATION

Aufbereitung der Berichtsergebnisse und Präsentation in einem Vor-Ort-Termin beim Auftraggeber oder als Webkonferenz.

II KONTINUIERLICHE DIENSTLEISTUNGEN

BESCHREIBUNG

INFORMATIONSSICHERHEITSBEAUFTRAGTER (ISB)

Bestellung zum Informationssicherheitsbeauftragten für Ihr Unternehmen und Wahrnehmung aller gesetzlich damit verbundenen Aufgaben. Die Grundlage für die Tätigkeit bildet die Implementierung eines branchenspezifischen Managementsystems für Informationssicherheit (ISMS) und der Aufbau einer Informationssicherheits-Organisation beim Auftraggeber. Inkludierte Zusatzleistungen sind die regelmäßige Bereitstellung von Fachinformationen, das Vorgehen nach unserem „Strukturierten Betreuungsprozess" sowie der Erhalt der Vitalfunktionen des ISMS.

BESCHREIBUNG

GAIMS

Webbasiertes Software-Tool zur Unterstützung des Aufbaus einer geeigneten internen Informationssicherheits- und/oder Datenschutz-Organisation und der Implementation eines Informationssicherheits- und/oder Datenschutz-Managementsystems (DSMS) auf Grundlage des BSI-Grundschutz, ISO27001 bzw. DSGVO und des BDSG-neu (oder entsprechender für den Auftraggeber geltende
Gesetze) in der Firmenorganisation des Auftraggebers.

5.4 PHASE 3: DAS PROJEKT-CONTROLLING

BESCHREIBUNG

INFORMATIONSSICHERHEITS-AUDIT

Planung und Durchführung von Informationssicherheits-Audits in der Organisation des Auftraggebers. Dokumentation und Zusammenfassung der Abweichungen in einem Management-Bericht und Bewertung möglicher Risiken.

BESCHREIBUNG

ÜBERPRÜFUNG DER INFORMATIONSSICHERHEITS-AUDITS

Sichtung und Bewertung vorliegender Dokumentationen und Berichte und die Durchführung eines aktuellen Maßnahmenabgleichs zu durchgeführten Audits zur Informationssicherheit.

CHECKLISTE: INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM AUFBAUEN UND STETIG ANPASSEN

RISIKO ASSESSMENT

- Bestimmung eines Scopes
- Interview/Workshop
- Zieldefinition
- Evaluierung der Verantwortlichkeiten
- Dokumentation und Aufbau eines Vorgehensmodells
- Definition weiterer Vorgehen/Maßnahmen

POLICY-ERSTELLUNG

- Zusichern von Management Attention
- Benennung ISB

BESCHREIBUNG DES ISMS

- Strukturierung und Beschreibung der Prozesse des ISMS
- Dokumentation von relevanten Schritten

ERMITTLUNG DES SCHUTZBEDARFS

- Eruierung von genutzen Systemen und Diensten
- Klassifizierung und Bewertung von Systemen und Daten
- Darstellung potenzieller Risiken für die einzelnen Systeme

MAßNAHMENABGLEICH

- Ausführliche Ist-Analyse nach bewährten Standards (z.B. ISO 27001/BSI Grundschutz)
- Risikoanalyse
- Maßnahmenableitung
- Handlungsempfehlungen
- Ergebnisdokumentation

RISIKOMANAGEMENT

- Planung und Durchführung von Maßnahmen
- Maßnahmentracking
- Durchführung von internen und externen Audits
- Akzeptanz des Restrisikos

BEGLEITENDE MAßNAHMEN

- Awareness-Schulungen
- Penetration-Tests
- Social-Engineering
- ISMS-Software (GAIMS)
- Audits

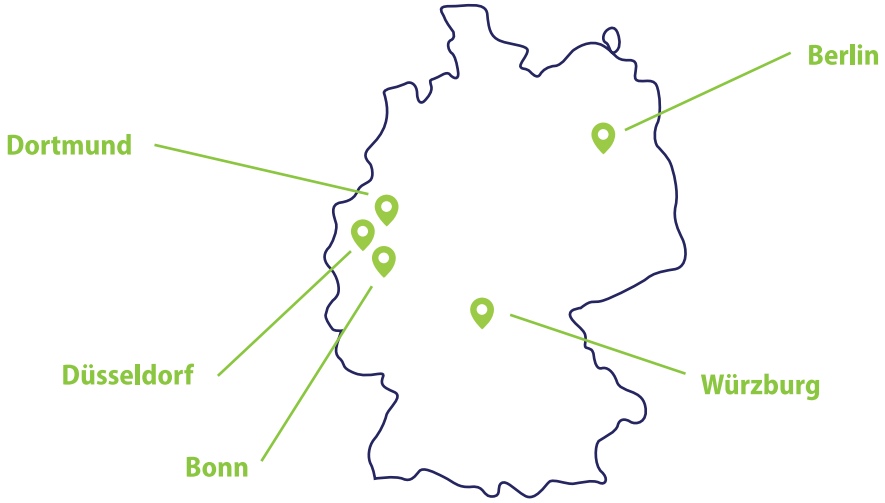
Sie benötigen weiterführende Informationen und Herangehensweisen zum Aufbau Ihres ISMS? Sprechen Sie uns an.

6. DATATREE AG - IHR PARTNER FÜR INFORMATIONSSICHERHEIT FÜR DAS KHZG

DATATREE

6. DATATREE AG – IHR PARTNER FÜR INFORMATIONS-SICHERHEIT FÜR DAS KHZG

Die DATATREE AG und ihre Experten mit Standorten in Berlin, Düsseldorf, Dortmund, Bonn und Würzburg bietet seit 2011 eine umfassende Beratung in den Bereichen Compliance, Datenschutz und Informationssicherheit.



Sie berät und unterstützt öffentliche sowie nicht-öffentliche Stellen bei der Einführung von Datenschutzmanagementsystemen sowie Managementsystemen für Informationssicherheit nach bewährten Standards und gesetzlichen Grundlagen. Neben Kunden im Einzelhandel, aus der Softwareentwicklung und der Kirche hat die DATATREE AG mit dem ISDSG, dem Institut für Sicherheit und Datenschutz im Gesundheitswesen, einen weiteren Schwerpunkt, der bereits auf jahrelange Erfahrung im Bereich Fort- und Weiterbildung sowie auch Vorträge, Magazine, Buchveröffentlichungen und Forschungsprojekten basiert.

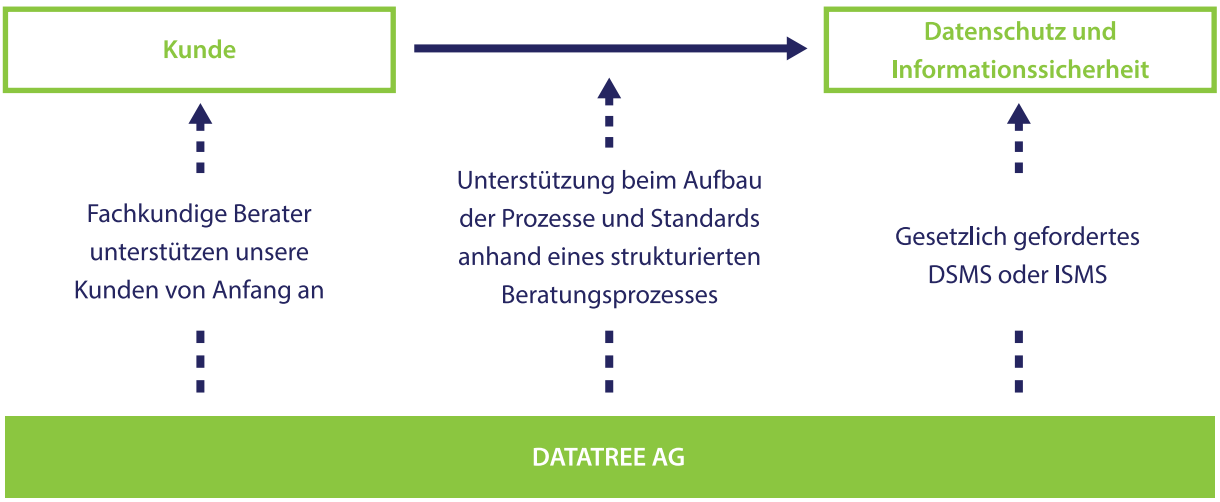
Die Tätigkeitsfelder des Compliance Providers umfassen die Themenfelder:

- Compliance
- Datenschutz
- Informationssicherheit
- Akademie
- Software für Managementsysteme

Datenschutz und Informationssicherheit

Die DATATREE bietet Beratung für Datenschutz und Informationssicherheit auf höchstem Niveau und unterstützt Unternehmen bei dem Aufbau ihrer Prozesse und Standards in Form eines gesetzlich geforderten Datenschutz-Managementsystems (DSMS) oder Informationssicherheitsmanagementsystem (ISMS) und den damit einhergehenden Aufgaben. Um den unterschiedlichen Anforderungen, gemessen an den Ist-Ständen, ihrer Kunden gerecht zu werden, hat die DATATREE ein eigenes Vorgehensmodell (Strukturierter Beratungsprozess), orientiert an etablierten Standards (QM-Management, ISO27001, Wirtschaftsprüfern), entwickelt, das eine optimale Integration in bereits bestehende Management-Systeme und maximale Flexibilität in Bezug auf die Entwicklung der eigenen Unternehmensprozesse durch den modularen Aufbau und den minimalen Einsatz von Ressourcen ermöglicht.

Der strukturierte Betreuungsprozess wird von fachkundigen Beratern gesteuert, die aufgrund ihrer Branchenkenntnisse die Geschäftsprozesse ihrer Kunden ganzheitlich, lösungsorientiert und pragmatisch analysieren, um gemeinsam mit den Kunden ein passgenaues Managementsystem für Datenschutz und/oder Informationssicherheit für ihr Unternehmen zu entwickeln und zu implementieren. Darüber hinaus bringt die DATATREE auch regelmäßig ihr Know-how in Forschungsprojekte ein.



UNSERE VERBUNDUNTERNEHMEN

DATATREE
YOUR COMPLIANCE PROVIDER

DIGITAL AVANTGARDE

GAIMS
Information Security

DR. JÄSCHKE
DIGITALISIERUNG

luugoo

<develop2grow>
making digital work

MEMO GMBH

Besuchen Sie unsere kostenlosen
Informationveranstaltungen

Vereinbaren Sie Ihren
individuellen Beratungstermin

Buchen Sie Ihren
Klinik-Workshop

Werden Sie Teil unseres Expertencircles auf LinkedIn
(inkl. wöchentlicher Roundtables)

und nehmen Sie das
KHZG jetzt in die Hand

Richten Sie Ihre Anfrage unverbindlich direkt an

khzg@datatree.eu

IMPRESSUM

ExperSite 01 2021 I ISSN-Print 2364-5636 I ISSN-Internet 2364-5644 I Herausgeber: Dr. Jäschke AG, Märkische Straße 212-218, 44141 Dortmund, T +49 231 9641930, F +49 231 964193-99, office@dr-jaeschke.ag, www.dr-jaeschke.ag I Redaktion, Design und Umsetzung: memo GmbH I Druck Druckerzeugnisse Gerbrunn I Auflage 5000 I Foto: S.3: Tom Schulte I Grafiken/Abbildungen: S.11: Abbildung in Anlehnung an die Grafik des Bundesamtes für Gesundheit, S.16: Abbildung in Anlehnung an die Grafik der Digital Avantgarde GmbH

DATATREE