Kontrollaufgaben des Datenschutzbeauftragten

5.5.2023

Fachtagung Datenschutz im Gesundheitswesen

Referentin

Nadja Köhler

Über mich

Konzerndatenschutzbeauftragte in einem Gesundheitskonzern, Leitung Stabstelle Konzerndatenschutz

Studium Public Management, Sozialrecht und Sozialwirtschaft, Europ. Arbeits- und Sozialrecht

Zert. Datenschutzbeauftragte

Externe Beraterin, DSB und Referentin für Datenschutz und Sozialrecht

Stellv. Sprecherin des Arbeitskreis Medizin (BvD)

Rahmenbedingungen der DSGVO

- Aufgaben nach Art 39 DSGVO
- Rechenschaftspflichten des Verantwortlichen
- Kontrollaufgaben des Verantwortlichen

Datenschutzorganisation

- Zeitpunkt der Kontrollen
- Kontrollen in der Datenschutzorganisation
- Beispiele von Kontrollen

Planung und Durchführung von Audits

- Auditphasen
- Auditplanung
- Auditdurchführung

Aufgaben des DSB – Art 39 DSGVO

Abs. 1 lit b) Überwachung der Einhaltung der DSGVO** sowie **Strategien

- *des **Verantwortlichen** oder des **Auftragsverarbeiters** für den Schutz personenbezogener Daten*
- ***Überprüfungen** von Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter*

➢ Strategien bzw. Regeln und Richtlinien, die sich Unternehmen oder Behörden selbst auferlegen. Hierzu können z.B. Unternehmensstrategie, BSC, Projekte, Prozesse, Betriebsvereinbarungen, Handlungsanweisungen, Dienstvereinbarungen, Industriestandards, Code of Conducts usw. gehören.

Abs. 1 lit c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und **Überwachung ihrer Durchführung** gemäß Artikel 35;

Art 38 DSGVO

- ***Abs. 6*** Der Datenschutzbeauftragte kann **andere Aufgaben und Pflichten** wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Aufgaben des DSB

Erwägungsgrund 97 DSGVO

„ In Fällen, […] wenn die Kerntätigkeit in der ***umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten besteht*** *[…] sollte der Verantwortliche oder der Auftragsverarbeiter bei* ***der Überwachung der internen Einhaltung der Bestimmungen*** *dieser Verordnung von einer weiteren* ***Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden“***

- Im Gesundheitswesen sollte der Verantwortliche bei der Überwachung der internen Einhaltung der DSGVO unterstützt werden

- z. B. durch einen DSB oder DS-Fachkundige Person

Aufgaben des DSB

Risikobasierter Ansatz Art 39 Abs. 2

Der DSB nimmt seine Aufgaben nach Art. 39 Abs. 2 DS-GVO **risikoorientiert wahr**. Er 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.

- Durchführung einer **eigenen Risikoeinschätzung** zur Berücksichtigung des mit den Verarbeitungsvorgängen verbundenen Risikos bei der Erfüllung seiner Aufgaben

- Kenntnis der Verfahren und Datenverarbeitung Voraussetzung

Befugnisse des DSB

- **EDSA Leitlinie Workingpaper 243* (ab S. 20 ff)**

Im Rahmen dieser Überwachungspflicht sind **DSB insbesondere befugt**,

- ✓ **Informationen** zur Ermittlung von Datenverarbeitungstätigkeiten zu **sammeln**,
- ✓ die Einhaltung der Vorgaben bei Datenverarbeitungstätigkeiten zu **analysieren** und zu **kontrollieren**,
- ✓ den Verantwortlichen oder den Auftragsverarbeiter zu **unterrichten** und zu **beraten** und ihm **Empfehlungen zu unterbreiten**.

Überwachung der Einhaltung **bedeutet nicht, dass der DSB im Fall der Nichteinhaltung persönlich zur Verantwortung** gezogen werden kann. Aus der DSGVO geht klar hervor, dass es Sache des Verantwortlichen – und nicht des DSB – ist, „geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“ (Artikel 24 Absatz 1). Die Einhaltung der datenschutzrechtlichen Bestimmungen fällt somit in den Aufgabenbereich des Verantwortlichen und nicht in den des DSB.

***https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf**

Gegenstand der Kontrollaufgaben

- Anwendungsbereich der DSGVO, andere Datenschutzvorschriften der EU und Mitgliedstaaten
- Erfüllung der Pflichten aus DSGVO und Datenschutzrecht sowie interner Regelungen / Strategien
- des Verantwortlichen oder Auftragsverarbeiters / keine Dritte
- Ganz / teilweise automatisierte Datenverarbeitungen sowie nichtautomatisierte Datenverarbeitungen, die in einem Dateisystem gespeichert sind
- ordnungsgemäße Anwendung der elektronischen Datenverarbeitung und analoge Prozesse
- Prozesse / Verfahren / Dokumente / Datenverarbeitungsprogramme / Systeme
- Keine Kontrollpflichten bei persönlicher oder familiärer Tätigkeiten durch natürliche Personen / Mitarbeiterexzess → Ausschluss von Kontrolle in Privatwohnungen / Regelung erforderlich
- Organisations- oder Verfahrensanweisungen, Richtlinien, Dokumentationen, TOM, Datenschutz durch Technik, Voreinstellungen, Schulungen/Sensibilisierungsmaßnahmen,
- Zuordnung von Zuständigkeiten und Wahrnehmung von zugeteilten Aufgaben
- Ordnungsgemäße Durchführung der DSFA

Überwachen gem. BvD Berufsbild des DSB*

Überwachen	Art. 39 ErwGr 81	• Risikoorientierte Festlegung datenschutzrelevanter Prüfungen • Veranlassen, begleiten oder durchführen von Auditierungen und Prüfungen inkl. erforderlicher Dokumentation • Überwachung der Prüfungen ◦ der datenverarbeitenden Geschäftsprozesse und Regelungen ◦ von IT-Systemen ◦ der datenschutzrelevanten Verträge ◦ der Dokumentation von Verarbeitungsvorgängen inkl. deren Risiko, insbesondere des Verzeichnisses von Verarbeitungstätigkeiten ◦ der Angemessenheit und Einhaltung der technischen und organisatorischen Maßnahmen ◦ von Verfahren, die einer Datenschutz-Folgenabschätzung unterliegen ◦ von Garantien externer Dienstleister (Auftragsverarbeiter) • Überwachung der Bearbeitung von Beschwerden und sicherheitsrelevanten Vorfällen

*** S. 30 https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf**

Dokumentation

- Zum eigenen Nachweis der Tätigkeiten / Enthaftung

- **DIIR Checkliste**: 3.1.3 Anforderungen an DSB „regelmäßiges Reporting“ (Dokumentation)

- z. B. **IDW Standard:** Zur Erfüllung der Rechenschaftspflicht: Dokumentation des DSB über wesentliche Tätigkeiten seiner Person, bzw. seiner Mitarbeiter in einem zentralen Dokumentationstool (IDW PH 9.860.1 für Prüfungen nach DSGVO und BDSG)

- Angelehnt an den **IDW Compliance Standard IDW PS 980: Dokumentation**

- Datenschutz-Kultur,
- Datenschutz-Ziele,
- Datenschutz-Risiken,
- Datenschutz-Programm,
- Datenschutz-Organisation,
- Datenschutz-Kommunikation,
- Datenschutz-Überwachung und - Verbesserung sowie viele wichtige Gestaltungshinweise.

Rechenschaftspflichten nach DSGVO

Kontrolle der Einhaltung der Grundsätze bei der Datenverarbeitung

- **Art 5 Abs. 2 DSGVO:** Pflicht zur Sicherstellung (=Kontrolle) der Einhaltung der Grundsätze
- Der für die Verarbeitung **Verantwortliche** muss die Einhaltung der Datenschutz-Grundsätze **nachweisen** können

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität & Vertraulichkeit

➢ **Originäre Pflicht des Verantwortlichen, kann aber auf DSB delegiert werden**

➢ **Pflicht zur Überprüfung der Einhaltung der Wirksamkeitskontrollen des Verantwortlichen**

➢ **z. B. Überprüfung anhand des VVT / Datenschutzkonzepte / Prüfberichte**

Rechenschaftspflichten nach DSGVO

Kontrolle der Einwilligungen

Art 7 Abs. 1 DSGVO:

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen können**, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

- **Kontrolle der Einholung von Einwilligungserklärungen / Nachweise**
- **Kontrolle der Einhaltung der Anforderungen an Einwilligungen**

Rechenschaftspflichten nach DSGVO

Führen eines Verzeichnis von Verarbeitungstätigkeiten

Art 30 DSGVO:

(1) Jeder Verantwortliche oder Auftragsverarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeit; Pflichtinhalte beachten

(2) Schriftich oder elektronisch zu führen

Kontrollaufgaben des Verantwortlichen

Kontrolle von Technischen und organisatorischen Maßnahmen auf Wirksamkeit

Art. 24 Abs. 1 DSGVO:

Der Verantwortliche setzt unter Berücksichtigung der Art und des Umfangs,

- der Umstände,
- der Zwecke der Verarbeitung,
- sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten
- geeignete technische und organisatorische Maßnahmen um und **überprüft diese**

➢ Prüfung geeigneter TOM

➢ Prüfung der Überprüfungen der Wirksamkeit der TOM

Kontrollaufgaben des Verantwortlichen

Kontrolle von Technischen und organisatorischen Maßnahmen auf Wirksamkeit

Art. 32 Abs. 1 DSGVO:

technischen und organisatorischen Maßnahmen nach dem **Stand der Technik**, dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessene Maßnahmen

Abs.1 d) ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen**

- Prüfung der TOM nach Stand der Technik
- Prüfung der Prozesse zur regelmäßigen Überprüfung der TOM

Kontrollaufgaben des Verantwortlichen

Kontrolle von Auftragsverarbeitungsverhältnissen

Art 28 Abs. 1 DSGVO: Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, **die hinreichend Garantien dafür bieten**, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den **Anforderungen dieser Verordnung** erfolgt und den **Schutz der Rechte** der betroffenen Person gewährleistet.

Art 28 Abs. 3 lit h: dem Verantwortlichen alle erforderlichen **Informationen zum Nachweis der Einhaltung** der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und **Überprüfungen** – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Art 29: Der **Auftragsverarbeiter** und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung des Verantwortlichen** verarbeiten

- Prüfung der Auftragsverarbeiter hinsichtlich geeigneter Garantien
- Prüfung der AVV selbst
- Prüfung der Einhaltung der Weisungen

Kontrollaufgaben des Verantwortlichen

Kontrolle von Drittlandübermittlungen

Art 44 DSGVO: Jedwede Übermittlung personenbezogener Daten an ein Drittland ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten

Kontrolle der Gültigkeit von Datenübermittlung aufgrund Angemessenheitsbeschluss

Kontrolle angemessener Garantien im Drittstaat bzw. durch den eingesetzten Auftragsverarbeiter

Mitwirkungspflicht des Verantwortlichen

- Datenschutzbeauftragte ist in Ausübung seiner Tätigkeit weisungsfrei
- Verantwortliche hat ihn bei der Erfüllung seiner Aufgaben zu unterstützen und Ressourcen zur Verfügung zu stellen
- insbesondere auch Ansprechpartner, Hilfspersonal, Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.
- Zutrittsrechte einräumen, Informationen bereitstellen
- Mitarbeiter müssen Auskünfte erteilen und notwendige Informationen bereitstellen
- Ressourcen für Weiterbildung und Erhalt der Fachkunde, Informationsbeschaffung

Rahmenbedingungen der DSGVO

- Aufgaben nach Art 39 DSGVO
- Rechenschaftspflichten des Verantwortlichen
- Kontrollaufgaben des Verantwortlichen

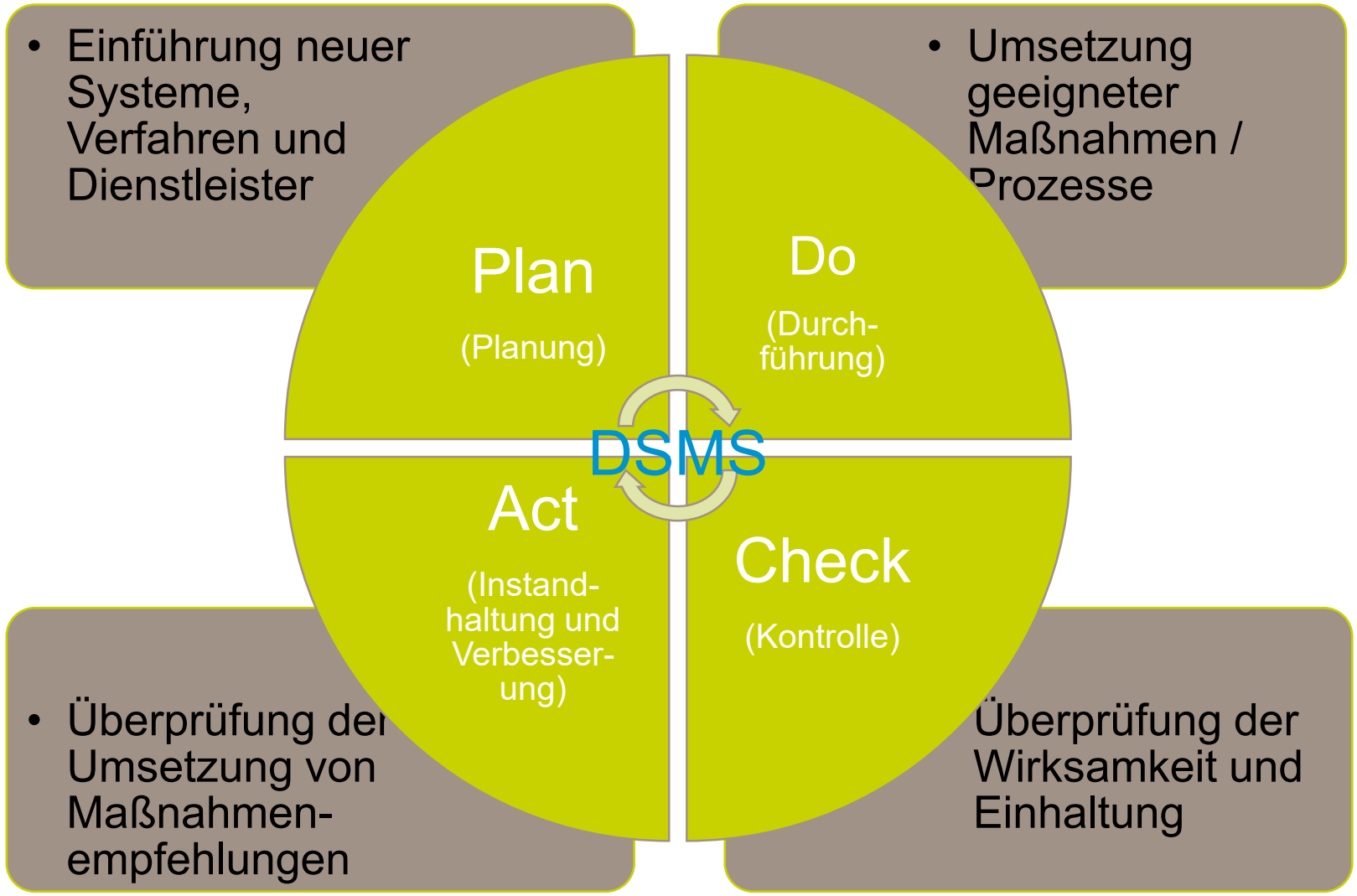
Datenschutzorganisation

- Zeitpunkt der Kontrollen
- Kontrollen in der Datenschutzorganisation
- Beispiele von Kontrollen

Planung und Durchführung von Audits

- Auditphasen
- Auditplanung
- Auditdurchführung

Zeitpunkt der Kontrollaufgaben



Arten von Kontrollen

- Anlasslose vs. Anlassbezogene Kontrolle
- Regelkontrolle vs Anlass-Kontrolle
- Standort, Entität, Unternehmensbereich, Prozesse/Verfahren, Software, Hardware, Dienstleister, Risikoklassifizierung, Art der Daten
- Stichprobenkontrolle vs. Allgemeine Kontrolle
- Vor-Ort-Kontrolle vs. Abstrakte Prüfung Dokumentenprüfung/Interviewbasierte Kontrolle
- Verantwortlicher vs. Auftragsverarbeiter
- Eigene Kontrolle vs delegierte Kontrollen
- Externe und interne Audits
- Second Party Audit / Third Party Audits

Kontrolle bei Einführung von Systemen/Verfahren

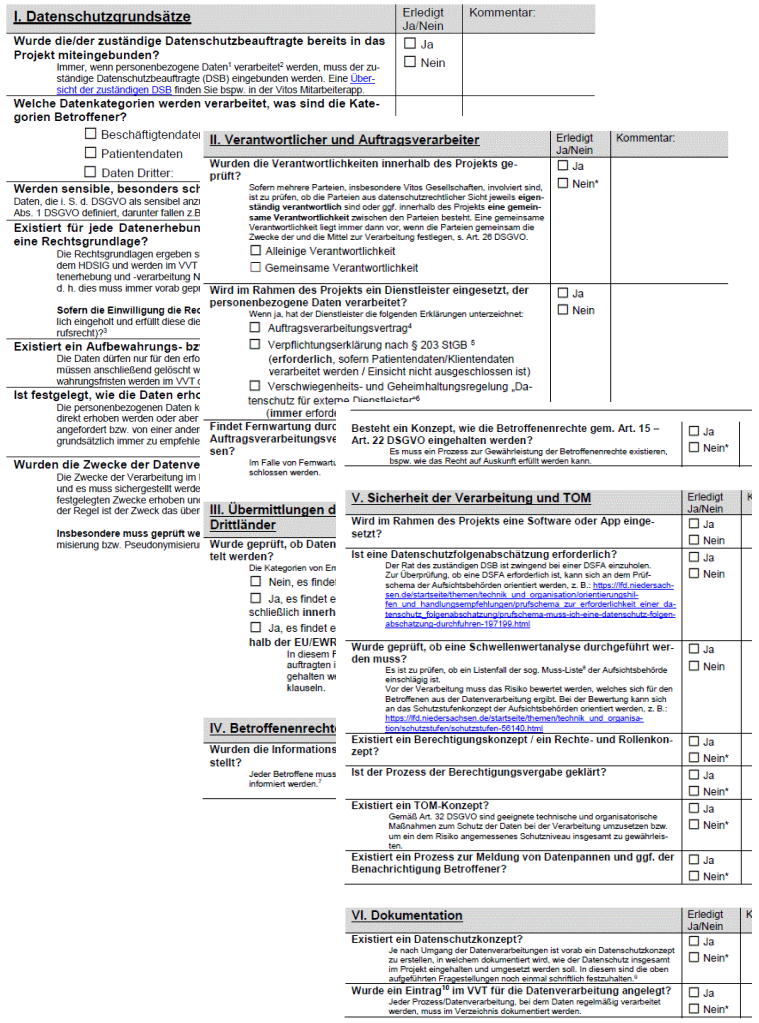
- Frühzeitige Einbindung bei der Planung der Einführung von neuen Verfahren und Systemen
- Regelmäßiger Austausch zur Geschäftsstrategie / IT Strategie
- Einbindung in Projektmanagement / Schnittstellenmanagement
- Implementierung im Prozess zur Einführung neuer Systeme
- IT Einkauf / Vergabe / Rechtsabteilung
- Gremienbeteiligung
- Kollektivvereinbarungen zur Einführung neuer IT Systeme
- Enge Schnittstelle zu Qualitätsmanagement / Prozessmanagement / Unternehmensentwicklung / Digitalisierung / IT
- Prüfung von Software und Dienstleister vor deren Vertragsschluss
- Einbeziehung im Ausschreibungsverfahren

Kontrolle bei Einführung von Systemen/Verfahren

Beispiel: Datenschutz in Projekten anhand von Checklisten

→ Arbeitspaket Datenschutz implementieren

- Checkliste zur Orientierung für Projektleitung
  - ✓ Einbindung DSB
  - ✓ Anwendungsbereich DSGVO
  - ✓ Art der Datenkategorien
  - ✓ Rechtmäßigkeit / Grundsätze
  - ✓ Betroffenenrechte
  - ✓ Einbindung Dienstleister (AVV, NDA, Drittlandübermittlung)
  - ✓ Einsatz Software (Anforderungen an Sicherheit)
  - ✓ Sicherheit der Verarbeitung / Risiko / TOM
  - ✓ Rechte- und Rollenkonzept
  - ✓ Aufbewahrungs-/Löschkonzept
  - ✓ Dokumentation DSGVO (Konzept, VVT)



I. Datenschutzgrundsätze | Erledigt Ja/Nein | Kommentar:

Wurde die/der zuständige Datenschutzbeauftragte bereits in das Projekt miteingebunden?
Immer, wenn personenbezogene Daten[1] verarbeitet[2] werden, muss der zuständige Datenschutzbeauftragte (DSB) eingebunden werden. Eine Übersicht der zuständigen DSB finden Sie bspw. in der Vitos Mitarbeiterapp.
☐ Ja ☐ Nein

Welche Datenkategorien werden verarbeitet, was sind die Kategorien Betroffener?
☐ Beschäftigtendaten
☐ Patientendaten
☐ Daten Dritter:

Werden sensible, besonders sch
Daten, die i. S. d. DSGVO als sensibel anz
Abs. 1 DSGVO definiert, darunter fallen z.B

Existiert für jede Datenerhebun
eine Rechtsgrundlage?
Die Rechtsgrundlagen ergeben s
dem HDSIG und werden im VVT
tenerhebung und -verarbeitung N
d. h. dies muss immer vorab gepr

Sofern die Einwilligung die Rec
lich eingeholt und erfüllt diese die
rufsrecht)?[3]

Existiert ein Aufbewahrungs- bz
Die Daten dürfen nur für den erfo
müssen anschließend gelöscht w
wahrungsfristen werden im VVT

Ist festgelegt, wie die Daten erhc
Die personenbezogenen Daten k
direkt erhoben werden oder aber
angefordert bzw. von einer ander
grundsätzlich immer zu empfehle

Wurden die Zwecke der Datenve
Die Zwecke der Verarbeitung im
und es muss sichergestellt werde
festgelegten Zwecke erhoben un
der Regel ist der Zweck das über

Insbesondere muss geprüft we
misierung bzw. Pseudonymisieru

II. Verantwortlicher und Auftragsverarbeiter | Erledigt Ja/Nein | Kommentar:

Wurden die Verantwortlichkeiten innerhalb des Projekts geprüft?
Sofern mehrere Parteien, insbesondere Vitos Gesellschaften, involviert sind, ist zu prüfen, ob die Parteien aus datenschutzrechtlicher Sicht jeweils **eigenständig verantwortlich** sind oder ggf. innerhalb des Projekts **eine gemeinsame Verantwortlichkeit** zwischen den Parteien besteht. Eine gemeinsame Verantwortlichkeit liegt immer dann vor, wenn die Parteien gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, s. Art. 26 DSGVO.
☐ Alleinige Verantwortlichkeit
☐ Gemeinsame Verantwortlichkeit
☐ Ja ☐ Nein*

Wird im Rahmen des Projekts ein Dienstleister eingesetzt, der personenbezogene Daten verarbeitet?
Wenn ja, hat der Dienstleister die folgenden Erklärungen unterzeichnet:
☐ Auftragsverarbeitungsvertrag[4]
☐ Verpflichtungserklärung nach § 203 StGB [5] (**erforderlich**, sofern Patientendaten/Klientendaten verarbeitet werden / Einsicht nicht ausgeschlossen ist)
☐ Verschwiegenheits- und Geheimhaltungsregelung „Datenschutz für externe Dienstleister"[6] (**immer erforderlich**)
☐ Ja ☐ Nein

Findet Fernwartung durc
Auftragsverarbeitungsve
sen?
Im Falle von Fernwartu
schlossen werden.

III. Übermittlungen d
Drittländer

Wurde geprüft, ob Daten
telt werden?
Die Kategorien von Er
☐ Nein, es findet
☐ Ja, es findet e
schließlich innerh
☐ Ja, es findet e
halb der EU/EWR
In diesem F
auftragten i
gehalten w
klauseln.

IV. Betroffenenrecht

Wurden die Informations
stellt?
Jeder Betroffene muss
informiert werden.[7]

Besteht ein Konzept, wie die Betroffenenrechte gem. Art. 15 – Art. 22 DSGVO eingehalten werden?
Es muss ein Prozess zur Gewährleistung der Betroffenenrechte existieren, bspw. wie das Recht auf Auskunft erfüllt werden kann.
☐ Ja ☐ Nein*

V. Sicherheit der Verarbeitung und TOM | Erledigt Ja/Nein

Wird im Rahmen des Projekts eine Software oder App eingesetzt?
☐ Ja ☐ Nein

Ist eine Datenschutzfolgenabschätzung erforderlich?
Der Rat des zuständigen DSB ist zwingend bei einer DSFA einzuholen. Zur Überprüfung, ob eine DSFA erforderlich ist, kann sich an dem Prüfschema der Aufsichtsbehörden orientiert werden, z. B.: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/pruefschema_zur_erforderlichkeit_einer_datenschutz_folgenabschatzung/pruefschema-muss-ich-eine-datenschutz-folgenabschatzung-durchfuhren-197196.html
☐ Ja ☐ Nein

Wurde geprüft, ob eine Schwellenwertanalyse durchgeführt werden muss?
Es ist zu prüfen, ob ein Listenfall der sog. Muss-Liste[8] der Aufsichtsbehörde einschlägig ist.
Vor der Verarbeitung muss das Risiko bewertet werden, welches sich für den Betroffenen aus der Datenverarbeitung ergibt. Bei der Bewertung kann sich an das Schutzstufenkonzept der Aufsichtsbehörden orientiert werden, z. B.: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/sohutzstufen/schutzstufen-58140.html
☐ Ja ☐ Nein

Existiert ein Berechtigungskonzept / ein Rechte- und Rollenkonzept?
☐ Ja ☐ Nein*

Ist der Prozess der Berechtigungsvergabe geklärt?
☐ Ja ☐ Nein*

Existiert ein TOM-Konzept?
Gemäß Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zum Schutz der Daten bei der Verarbeitung umzusetzen bzw. um ein dem Risiko angemessenes Schutzniveau insgesamt zu gewährleisten.
☐ Ja ☐ Nein*

Existiert ein Prozess zur Meldung von Datenpannen und ggf. der Benachrichtigung Betroffener?
☐ Ja ☐ Nein*

VI. Dokumentation | Erledigt Ja/Nein

Existiert ein Datenschutzkonzept?
Je nach Umgang der Datenverarbeitungen ist vorab ein Datenschutzkonzept zu erstellen, in welchem dokumentiert wird, wie der Datenschutz insgesamt im Projekt eingehalten und umgesetzt werden soll. In diesem sind die oben aufgeführten Fragestellungen noch einmal schriftlich festzuhalten.[9]
☐ Ja ☐ Nein*

Wurde ein Eintrag[10] im VVT für die Datenverarbeitung angelegt?
Jeder Prozess/Datenverarbeitung, bei dem Daten regelmäßig verarbeitet werden, muss im Verzeichnis dokumentiert werden.
☐ Ja ☐ Nein*

Kontrolle bei Einführung von Systemen/Verfahren

Beispiel: Einbindung des DSB bei Ausschreibungsverfahren

→ Anforderungscheckliste

→ Beteiligung DSB bei Erstellung der Leistungsbeschreibung / Leistungsverzeichnis

→ Etablierung von Standarddokumenten für Ausschreibungen, z. B. NDA, AVV, Verpflichtungserklärungen, TOM, VVT nach Art 30 Abs. 2

→ Abschluss EVB-IT Verträge als Standard → beinhaltet ebenfalls Datenschutzpassagen

→ Festlegung von allgemeinen Anforderungen, z. B. Drittland

→ Beteiligung während der Ausschreibungsphase: Bieterfragen

→ Beteiligung bei Auswahlverfahren geeigneter Dienstleister / Software

Kontrolle bei Einführung von Systemen/Verfahren

Beispiel: Einbindung des DSB bei Ausschreibungsverfahren

Markterkundung	Bedarfs-feststellung	Leistungs-beschreibung	Angebot	Vertragsschluss
Was gibt es?	Was wollen wir?	So soll es sein!	Ist es das?	Das ist es!
Welche Datenschutz-konformen Anbieter / Systeme / Prozesse gibt es?	Einbindung DSB: DSGVO Konformität prüfen	Festlegung von DS-Anforderungen in Leistungs-beschreibung / Leistungsverzeichnis / Vorgabe Vertrags-bestimmungen / AVV / NDA	Angebotsprüfung / Dokumentenprüfung / Prüfung AVV / Subunternehmer / Drittland / TOM	Unterzeichnung aller Verträge Prüfung der Einhaltung der Leistungsanforderungen

Kontrolle der Umsetzung der DSGVO

- Überprüfung Pflichten aus DSGVO
- Überprüfung vorliegender Dokumente, z. B. Datenschutzleitlinie, Datenschutzrichtlinie, Datenschutzhandbuch, QMH, TOM
- Stichproben, z.B. Verpflichtungserklärung von Beschäftigten, Einwilligungserklärungen, AVV, NDA, Prüfung Schulungsquoten im Konzern; Zugriffsprotokolle
- Prüfung von Prozessen für Meldung Datenpannen, Umgang Betroffenenrechte, Einwilligung
- Kontrolle von KPI*: Datenschutzanfragen, Meldungen Art 33, Benachrichtigung Art 34, Anzahl Abschluss AVV, Joint Controller, Beschwerden Betroffener, Anzahl Geltendmachung Betroffenenrechte, Anfragen Aufsichtsbehörde

*KPI: Key Performance Indicators = Schlüsselkennzahlen

Kontrolle der Datenschutzorganisation

Normen zur Überprüfung der Datenschutzorganisation

- ISO 27701 i.V.m ISO 27001
- Branchenspezifischer Sicherheitsstandard Gesundheitswesen (B3S)
- Cloud C5 / ISO 27018
- IDW PS 380 (Wirtschaftsprüfer)
- Revision: Checkliste zur Prüfung der Datenschutzorganisation DIIR-Arbeitskreis Interne Revision & Datenschutz
- SDM (Standarddatenschutzmodell) sowie
- entsprechende Maßnahmenkataloge
- Checklisten von Aufsichtsbehörden
- ….

Bezeichnung
Baustein 11 „Aufbewahren“ (Version 1.0 vom 6. Oktober 2020)
Baustein 41 „Planen und Spezifizieren“ (Version 1.0 vom 25. März 2021)
Baustein 42 „Dokumentieren“ (Version 1.0a vom 2. September 2020)
Baustein 43 „Protokollieren“ (Version 1.0a vom 2. September 2020)
Baustein 50 „Trennen“ (Version 1.0 vom 6. Oktober 2020)
Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ (Version 1.0 vom 01.11.2021)
Baustein 60 „Löschen und Vernichten“ (Version 1.0a vom 2. September 2020)
Baustein 61 „Berichtigen“ (Version 1.0 vom 6. Oktober 2020)
Baustein 62 „Einschränken der Verarbeitung“ (Version 1.0 vom 6. Oktober 2020)

Beispiel: Kontrolle von Auftragsverarbeitern

Risikobasierte Überprüfung von Auftragsverarbeitern

- Regelmäßigen Turnus implementieren
- Fristlauf ab Zeitpunkt der Vertragsunterzeichnung AVV
- Risikobewertung des Auftragsverarbeiter aufgrund Abhängigkeit / Kernprozesse
- Kontrolle der Einhaltung der Regelungen im AVV zu eingesetzten Subunternehmer, Meldung Datenpannen und Betroffenenrechte, TOM, Zertifikate/Nachweise, Kontaktdaten DSB/Ansprechpartner für Weisungen
- Stichprobenkontrolle der Weisungen
- Vor-Ort-Kontrolle / Dokumentenprüfung / Fragebogen / Zertifizierungsberichte

Orientierung an Verhaltensregel: Trusted data processor

- Richtet sich auf datenschutzrechtliche Geschäftsprozesse als Standard
- Kriterienkatalog aus Trusted Data Processor ableiten

Kontrolle von IT / EDV-Systemen und Prozessen

- BSI IT Grundschutzkompenium
- Brachenspezifischer Sicherheitsstandard Gesundheitswesen (B3S)
- ISO 27001/27002/27701
- C5 Cloud
- ISO 27018
- OH KIS
- Richtlinie IT Sicherheit im MVZ § 75b SGB V
- BSI technische Richtlinie z. B. zur Verschlüsselung, Kryptografie

Kontrolle von IT / EDV-Systemen und Prozessen

Beispiel: Kontrolle von Rechenzentren (intern oder extern)

→ Besichtigung vor Ort

→ Aufwendig in Vorbereitung und Durchführung

→ Fokus: Überprüfung der angegebenen TOM

→ Dokumentenprüfen und Vor-Ort-Besichtigung der Räumlichkeiten

→ Prüfkatalog anhand BSI IT Grundschutz INF: Infrastruktur

- **INF.2 Rechenzentrum sowie Serverraum**
- **Ggf. Ergänzung um INF.5 Raum sowie Schrank für technische Infrastruktur**
- **Anforderungen bei erhöhtem Schutzbedarf beachten**
- **Vertragliche Regelungen beachten ggf. ergänzen**

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_2_Rechenzentrum_sowie_Serverraum_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

Kontrolle von IT / EDV-Systemen und Prozessen

Beispiel: Kontrolle der Umsetzung KIS Berechtigungskonzeptes

→ Orientierung an OH KIS

→ Scope: Dokumentenprüfung und Prüfung im System (Stichproben)

→ Vorbereitung anhand Fragebogen auf Basis OH KIS sowie Checkliste einzureichenden Unterlagen

→ Berechtigungsüberprüfung anhand von Berufsgruppen und Anmelderollen

z. B. Stationsarzt, Leitender Arzt, Pflegeperson, Pflegedienstleitung

Konsilanforderung, Vertretung, Notfallzugriff

Liste aller berechtigten Personen mit Personalliste abgleichen

Stichproben von Zugriffen ziehen (Begründungen überprüfen)

→ Achtung: Betriebsrat einbeziehen!

	Dokument/Anlagen	Liegt bei
1	Ausgefüllter Fragenkatalog	☐Ja ☐ Nein
2	Gesellschaftsbezogenen ausgefüllten KIS Berechtigungskonzept NG (Stand 22.4.2020)	☐Ja ☐ Nein
3	Ggf. Begründung für die Abweichungen von der kleinsten Organisationseinheit	☐Ja ☐ Nein
4	Beschreibung bzw. Erläuterung der Organisationsstruktur unter Nennung der jeweiligen Fachrichtungen, Fachbereichen. Betriebsstätten (z.B. Organigramm oder eine andere Übersicht)	☐Ja ☐ Nein
5	Ist-Berechtigungskonzept (Übersichtsmatrix der Anmelde-, Rechte- und Ermächtigungsrollen)	☐Ja ☐ Nein
6	Übersicht aller Nutzer, die Zugang zum KIS haben	☐Ja ☐ Nein
7	Übersicht der den Mitarbeitern zugeordneter Rollen	☐Ja ☐ Nein
8	Dokumentierter Prozess zur Vergabe, Änderung und Entzug von Berechtigungen im KIS	☐Ja ☐ Nein
9	Formular/Dokumentation, welches die wesentlichen bestehenden Rechte- und Anmelderollen zur Rechteerteilung enthält.	☐Ja ☐ Nein
10	Konzept, in welcher Form Stichprobenkontrollen durch wen in welchem Abstand in welcher Art und Weise durchgeführt wird und wer daran beteiligt ist.	☐Ja ☐ Nein
11	Festlegung, wer die regelmäßigen Stichproben. Protokollauswertung vornimmt und welche Stellen zu informieren sind und wie die Auswertungen und Ergebnisse zu dokumentieren sind.	☐Ja ☐ Nein
12	Regelung, inwiefern mit nachgewiesenen unberechtigten Zugriffen innerhalb der TG umgegangen wird und welche Folgen sich hieraus für den Beschäftigten ergeben.	☐Ja ☐ Nein
13	mehrstufiges, schriftliches Verfahren, welches die Freigabeprozesse definiert.	☐Ja ☐ Nein
14	zusätzliches Berechtigungskonzept für Zugriffe in Notfallsituationen	☐Ja ☐ Nein

Kontrolle von Gesundheitsanwendungen

- Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz*
- Sicherheitsanforderungen an digitale Gesundheitsanwendungen Technische Richtlinie BSI TR-03161[2]
- Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter
- Prüfnachweis Videosprechstunde nach § 365 SGB V Anlage 31b zum BMV-Ä sowie Auslegungshilfen[3]
- Checkliste „Datenschutzrechtliche Aspekte im Rahmen von Verträgen nach § 140a SGB V“

*https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.pdf;jsessionid=14C9E13414B6C0CB33614024C89B8533.intranet232?__blob=publicationFile

[2]https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/tr-03161.html

[3]https://www.datenschutz-cert.de/fileadmin/user_upload/Download-Center/Videosprechstunde/Auslegungshinweise_Videosprechstunden_VSS_20220701.pdf

Kontrolle von Datenaufbewahrung und -entsorgung

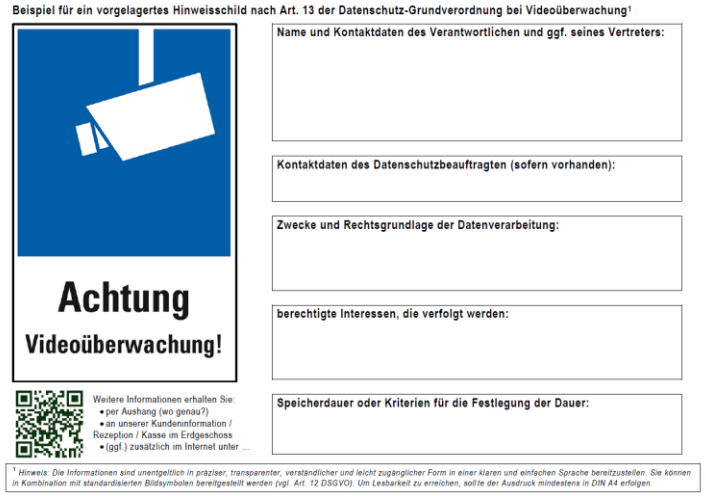
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten (DIN 66398)
- Vernichten von Datenträgern (DIN 66399)
- SDM Baustein 11 „Aufbewahren“
- SDM Baustein 60 „Löschen und Vernichten“

Kontrolle durch Begehungen

- Anhand von Begehungscheckliste
- Interviews mit Mitarbeitenden
- Beispielbereiche:
  - Stationsstützpunkt
  - Anmeldung
  - Zentrale Notaufnahme
  - Stationsflure
  - Arbeitsplätze / Büros
  - Archiv
  - Videoüberwachungen / Intensivstation

Kontrolle von Videoüberwachung

- DIN 33450 Hinweisschild Videoüberwachung / DIN 62676-4
- Erfassung aller Videoüberwachungen / Kamera
- Vorhandene Dokumentation prüfen (Rechtsgrundlage, VVT, DSFA)
- Blickwinkel der Kamera / Aufstellbereich (öffentlich, nicht-öffentlich)
- Aufzeichnung / Speicherung
- Aushang Informationspflichten / Kennzeichnung*
- Speicherdauer / Einsichtsrechte / befugte Personen
- Interessenabwägung



- https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf
- https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf
- *https://www.lda.bayern.de/media/muster/video_hinweis.pdf
- https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf

Kontrolle von Aktenaufbewahrung / Archiv

- Orientierung an ISO11799
  - Klima, Brandschutz, Schutz vor Hochwasser und Grundwasser,
- Archivordnung
- Zutrittsregelungen / Berechtigungen
- Einsicht von außen
- Art der Archivierung / Systematik / Aufbewahrungsfristen
- Umgang mit Fenster / Türen nach Feierabend
- Entsorgung
- Verschlossene Regale / Trennung von Archivgut
- Prozess zur Anforderung von Archivgut
- ggf. Zertifikate

Sonderfall Kontrolltätigkeiten Betriebsrat

§ 79a BetrVG

- **Betriebsrat als Teil der Verantwortlichen Stelle**
- **Kontrollrecht auch gegenüber Betriebsrat**
- **Besondere Geheimhaltungsverpflichtungen gegenüber Arbeitgeber**

Rahmenbedingungen der DSGVO

- Aufgaben nach Art 39 DSGVO
- Rechenschaftspflichten des Verantwortlichen
- Kontrollaufgaben des Verantwortlichen

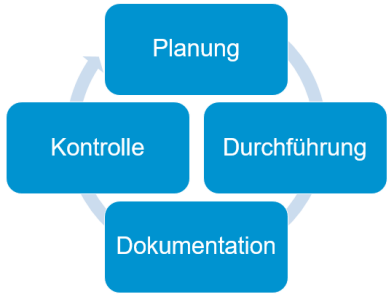
Datenschutzorganisation

- Zeitpunkt der Kontrollen
- Kontrollen in der Datenschutzorganisation
- Beispiele von Kontrollen

Planung und Durchführung von Audits

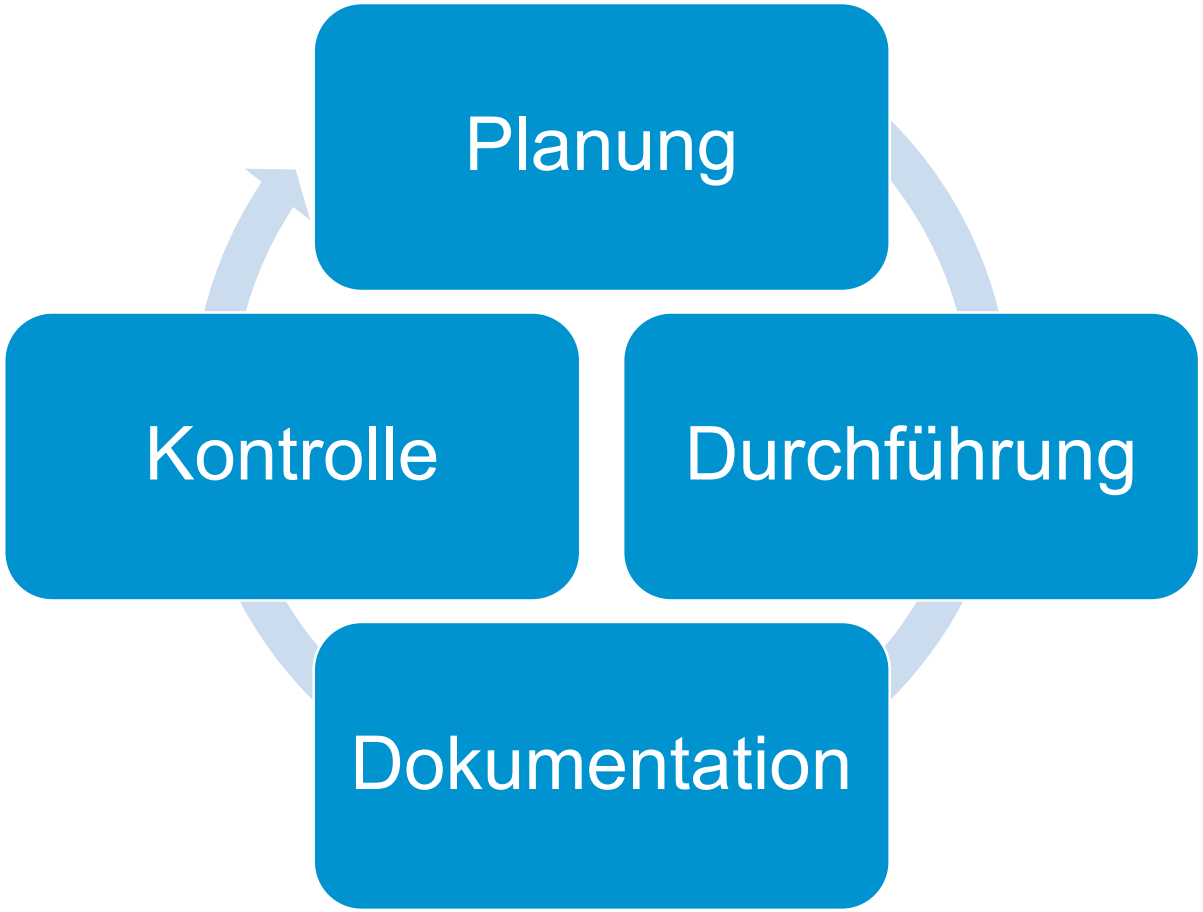
- Auditphasen
- Auditplanung
- Auditdurchführung

Audit als Nachweis der Einhaltung der DSGVO

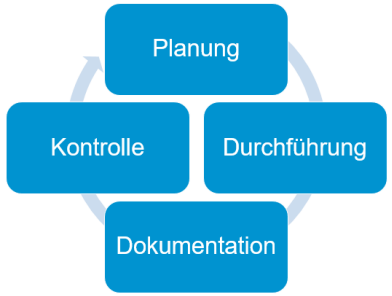


- Audits sind *„systematische , unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiven Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt werden“* (ISO 19011:2011 Leitfaden zur Auditierung von Managementsystemen)
- Rechenschaftspflichten als Grundlage verpflichtender Datenschutz-Audits
- DSGVO sieht keine strukturierten Audits vor, aber Nachweis der Einhaltung der DSGVO durch Audits
- Nachweis durch Verhaltensregeln und Zertifizierungen möglich (Art 40, 42 DSGVO)
- Mittelbar durch Kontrollpflichten des Verantwortlichen
- Audits können Haftungsrisiko / Bußgelder minimieren

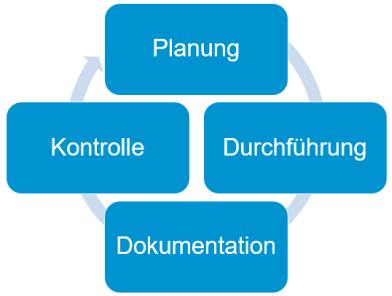
Prozessablauf von Audits



Audits - Planung



- Was: Festlegung des Prüfungsscopes
- Wann: Zeitplanung
- Wer: Ansprechpartner
- Wie: Ablauf, welche Methoden
- Wie oft: Auditplan / Auditprogramm



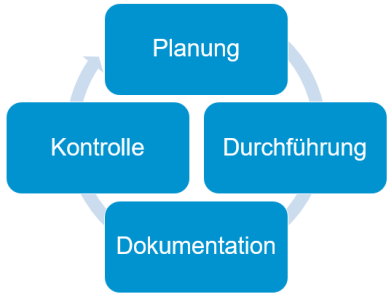
Audit – Kontrollbereiche

§ Recht: rechtliche Anforderungen der DSGVO

Organisation: datenschutzrechtliche Verantwortungsbereiche

Prozesse: datenschutzrechtliche Prozesse

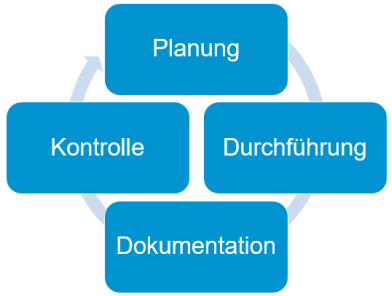
IT: Anforderungen an IT-Systeme, Datensicherheit



Auditplanung – Prüfungsscope

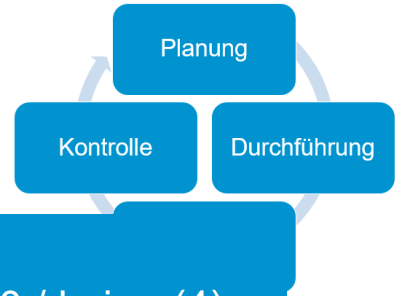
datenschutzorganisation
betriebsarzt
berechtigungskonzept
dienstleister
richtlinien
geschäftsbereich
dstenentsorgung
prozesse
räume
tom
it
zertifikate
datenerfassung
etc
personal
entities
datenweitergabe
rechenzentrum
software
hardware
av-verträge
schulungen
archiv
standort
videoüberwachung
begandlungsprozesse
auftragsverarbeiter
betriebsrat
datenschutzpannen
geschäftsprozesse
löschkonzept
betroffenenrechte
datenaufbewahrung

Audits – Risikofestlegung / Punktesystem



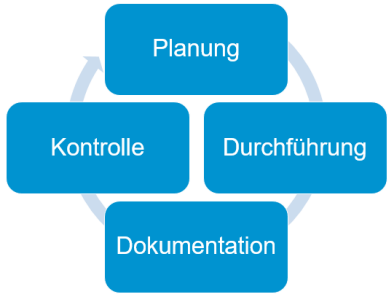
- Kernprozesse vs. unterstützende Prozesse
- Art der Datenkategorien und Risikoklassifizierung
- Umfang der Datenverarbeitung
- Umfang der betroffenen Personen
- Schwellenwertanalyse / DSFA
- Anzahl der Datenschutzmeldungen
- Letzter Zeitpunkt der Prüfung
- Ergebnis der letzten Prüfung
- Öffentlichkeitswirksamkeit
- …..

Audits – Punktesystem / Beispiel [Auszug]



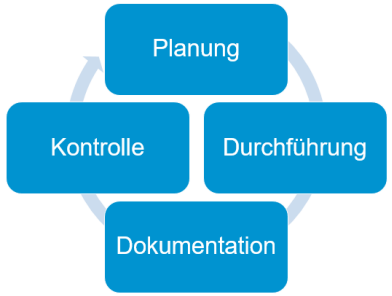
Zeitpunkt der letzten Prüfung	Weniger als 2 Jahre (1) 2 bis 5 Jahre (2) 5-10 Jahre (3) Länger als 10 / keine (4)
Art des Prozesses	Kernprozess (4) Unterstützende Prozesse (3) Nebenprozesse (2)
Daten-kategorie	Gesundheitsdaten (4) andere Art 9 (3) Art 6 (2) nur Kontaktdaten (1)
Ergebnis der letzten Prüfung	Keine Feststellung (0) Keine Prio1 (1) mind. 1 -2 Prio 1 (3) mehr als 2 Prio1 (4)
Ergebnis Schwellenwertnanalyse	Keine DSFA/gering (1) mittel (2) hoch (3) sehr hoch (4)

Audits – Risikoorientierte Prüfungsplanung



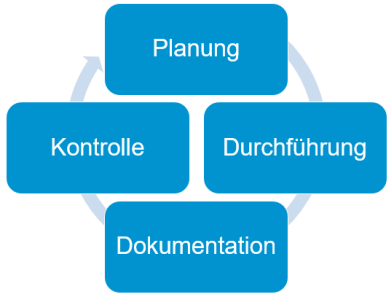
- Festlegung der Anzahl der jährlich durchzuführenden Prüfung anhand verfügbarer Kapazitäten
- Festlegung des Schwellenwerts (ab welcher Punktezahl)
- erreichte Wert entscheidet darüber, welche Prüffelder in der Prüfungsplanung priorisiert werden
- Festlegung des Prüfungszyklus

Audits – Durchführung



- Kick-Off (mit verantwortlicher Leitung)
- Durchführung gemäß Auditplan / Zeitplan
- Dokumentensichtung / Begehung/Augenscheinnahme / Beobachtung / Interview / Testergebnisse / Auswertungen / Stichproben
- Abschlussgespräch / Maßnahmenplanung
- Abschlussbericht

Audits – Audit Bewertung [Beispiel]



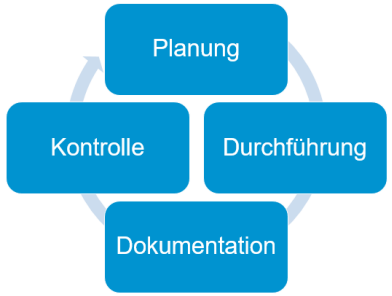
Priorität 1 — Es wird eine **gesetzliche Vorschrift nicht eingehalten** bzw. es besteht aktuell ein sehr hohes Risiko. Es sind umgehend Maßnahmen einzuleiten, um den Verstoß abzustellen.

Priorität 2 — Es wird eine **interne Vorgabe** nicht eingehalten. Die derzeitige Geschäftsabwicklung kann zu einem **hohen Unternehmensrisiko** führen.

Priorität 3 — Es wird eine **interne Vorgabe** nicht eingehalten. Mit der Nichteinhaltung ist ein **niedriges Unternehmensrisiko** verbunden.

Priorität 4 — Es sind **Verbesserungen/Empfehlungen** in der Unternehmensabwicklung möglich, diese sind bei einer Neugestaltung bzw. Änderung von Prozessen zu berücksichtigen.

Audits – Audit-Dokumentation



- Abschlussbericht mit Feststellungen / Begehungsprotokoll / Fotodokumentation / Checklistenbewertungen / Stellungnahmen
- Maßnahmen / Empfehlungskatalog mit Priofestlegung
- Umsetzungsplanung
- Auditbericht Abschlussgespräch
- Festlegung der Maßnahmenumsetzung einschließlich Zuständigkeiten
- Zeitrahmen
- Interne Dokumentation (Protokolle, Vermerke Bericht, bereitgestellt. Unterlagen)

Vielen Dank für die Aufmerksamkeit

Íhr Kontakt bei Rückfragen

Nadja Köhler

koehler@datenschutzmentor.com