Datenschutzkonzept
Erstellung und Umsetzung

§ 15 Abs. 4 KDG-DVO

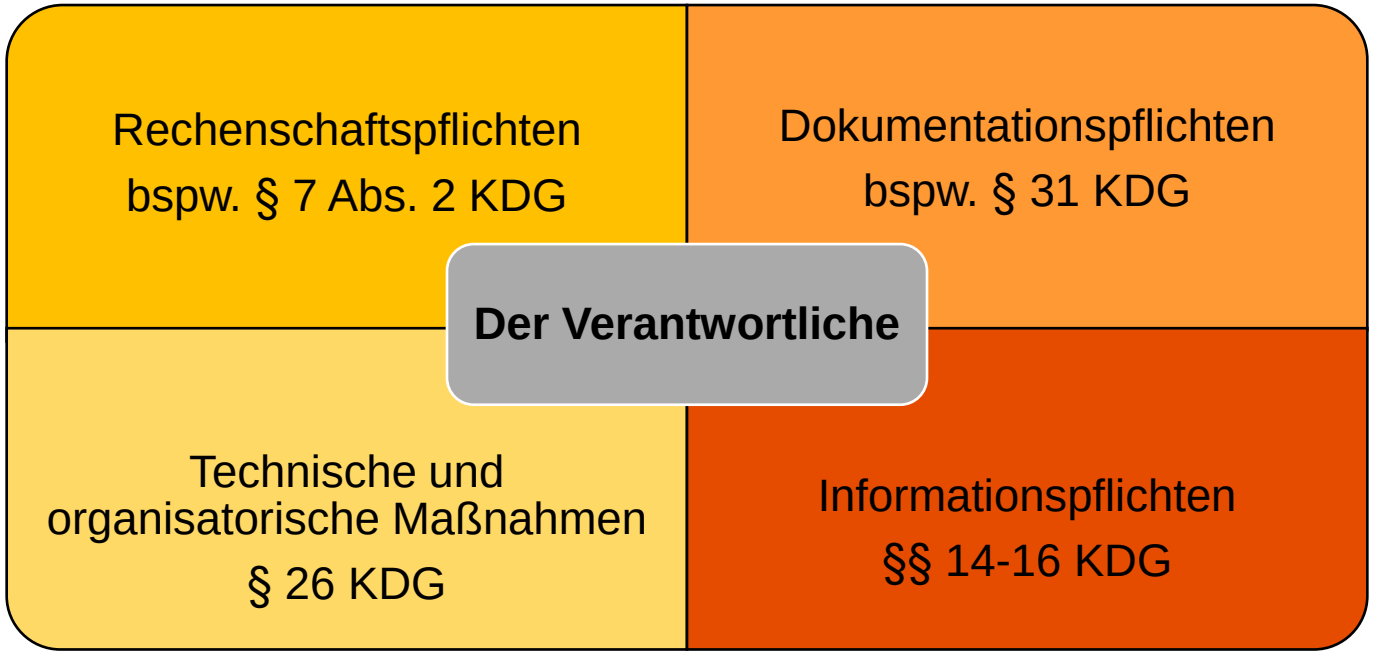
Diözese Rottenburg-Stuttgart

Datenschutz in der Diözese Rottenburg-Stuttgart

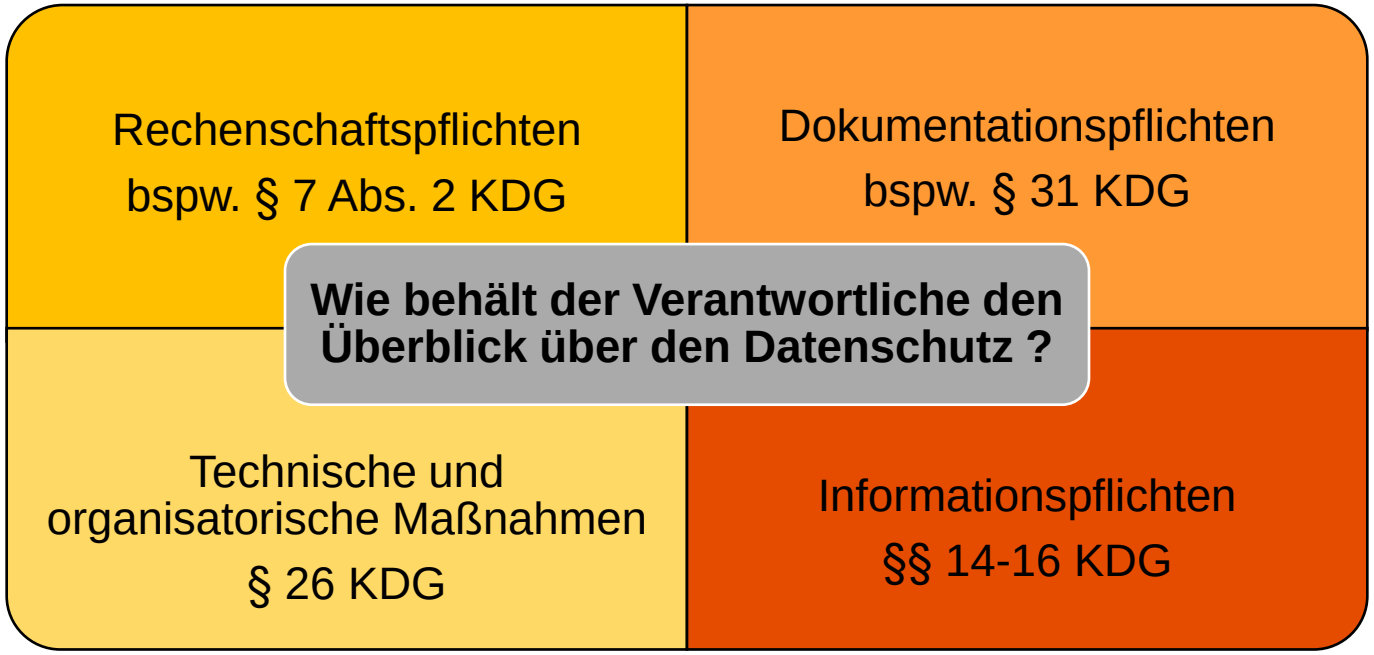
Agenda

I. Einführung
II. Das Datenschutzkonzept
III. Umsetzung in der Praxis
IV. Beispiele
V. Zusammenfassung

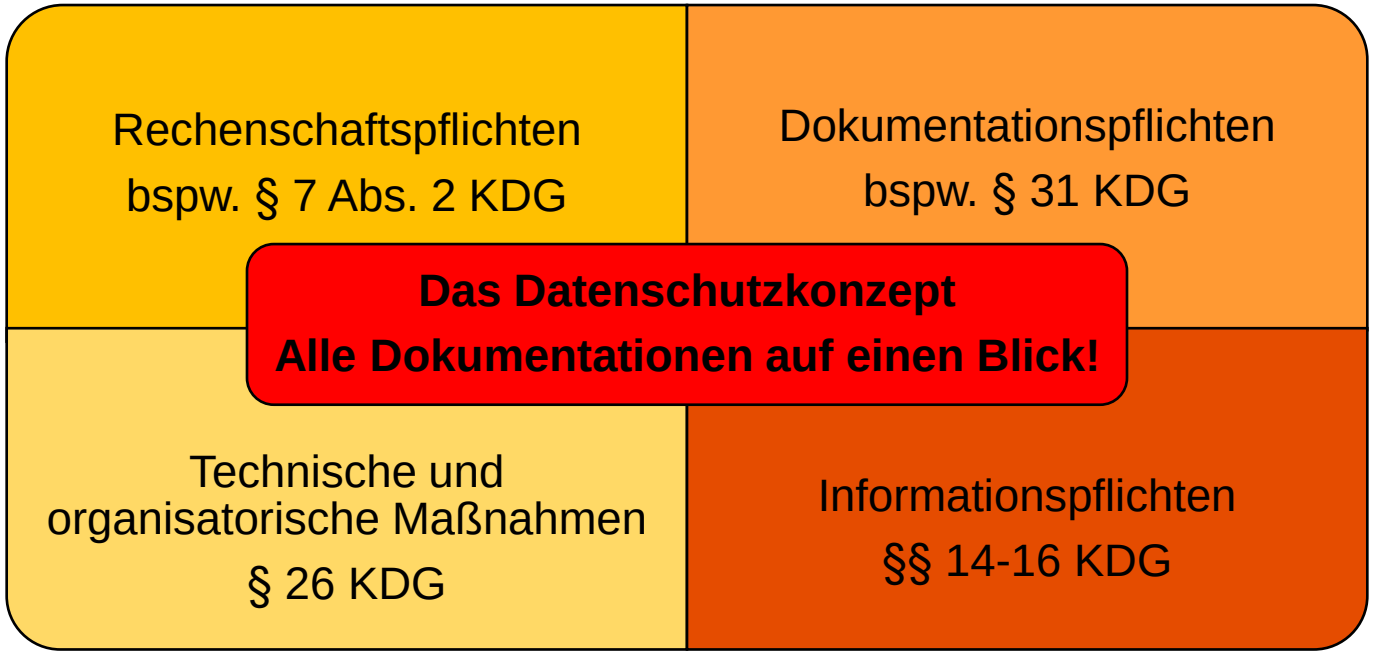
I. Einführung



I. Einführung



I. Einführung



II. Das Datenschutzkonzept

- Was ist ein Datenschutzkonzept?
  - Es ist eine Dokumentation, die einen Überblick über alle datenschutzrechtlichen Aspekte der verantwortlichen Stelle gibt.
  - Es umfasst alle datenschutzrechtlichen Aspekte der Einrichtung in einer Dokumentation und erfüllt dadurch die Dokumentations- und Rechenschaftspflichten aus dem KDG und der KDG-DVO.

- Wie funktioniert das Datenschutzkonzept?
  - Zunächst wird der **Ist-Zustand** dokumentiert.
  - Als zweites werden die Schritte zum rechtskonformen **Soll-Zustand** festgelegt.

II. Das Datenschutzkonzept

- Warum ist das Datenschutzkonzept wichtig?
  - § 15 Abs. 4 KDG-DVO schreibt die Erstellung und Umsetzung vor.
  - Es dient als Nachweis gegenüber der Datenschutzaufsicht.
  - **Das Datenschutzkonzept leistet einen Beitrag für einen hohen datenschutzrechtlichen Standard in Ihrer Einrichtung.**

II. Das Datenschutzkonzept

- Für wen findet das Datenschutzkonzept Anwendung?
  - Grundsätzlich für alle kirchlichen Stellen nach § 3 Abs. 1 lit. a) KDG. Diözese, Dekanate, (Gesamt-)Kirchengemeinden, Verwaltungszentren, Kindergärten, Sozialstationen
- Wer trägt für die Erstellung des Datenschutzkonzepts Sorge?
  - Grundsätzlich der Verantwortliche für den Datenschutz (z. B. Pfarrer und gewählte KGR-Vorsitzende, Dekan, VZ-Leitung).
  - Delegation an einrichtungsinterne Ansprechperson für das Thema Datenschutz ist möglich.
  - Bei Fragen zu technischen und organisatorischen Maßnahmen kann der Verantwortliche den IT-Partner hinzuziehen.

III. Umsetzung in der Praxis

Geltungsbereich

Für welche Einrichtung(en) findet das Datenschutzkonzept Anwendung?

Einrichtung / Organisationseinheit / Kirchengemeinde / Kindergarten
Beispiel: Verwaltungszentrum XY
Beispiel: Kirchengemeinde St. Martin
Beispiel: Sozialstation XY
Beispiel: Kindergarten Musterstadt

III. Umsetzung in der Praxis

Zuständigkeitsregelungen und Kontaktdaten

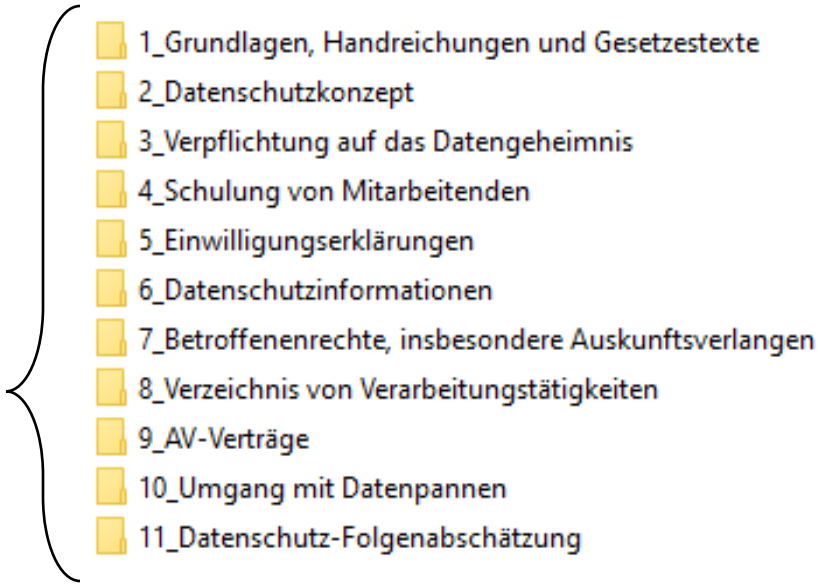
Zuständigkeitsbereich	Kontaktdaten
Verantwortlicher für den Datenschutz	
Einrichtungsinterne Ansprechperson für das Thema Datenschutz	
IT-Partner bzw. IT-Dienstleister	
Einrichtungsinterne Ansprechperson für das Thema IT und IT-Sicherheit	
Betrieblicher Datenschutzbeauftragter	Bischöfliches Ordinariat Stabsstelle Datenschutz Postfach 9 72101 Rottenburg Tel.: (0 74 72) 169-890 Fax: (0 74 72) 169-8 38 90 E-Mail: datenschutz@bo.drs.de

III. Umsetzung in der Praxis

Vorbereitung und Organisation (vgl. Nr. 4; S. 7 des DSK)

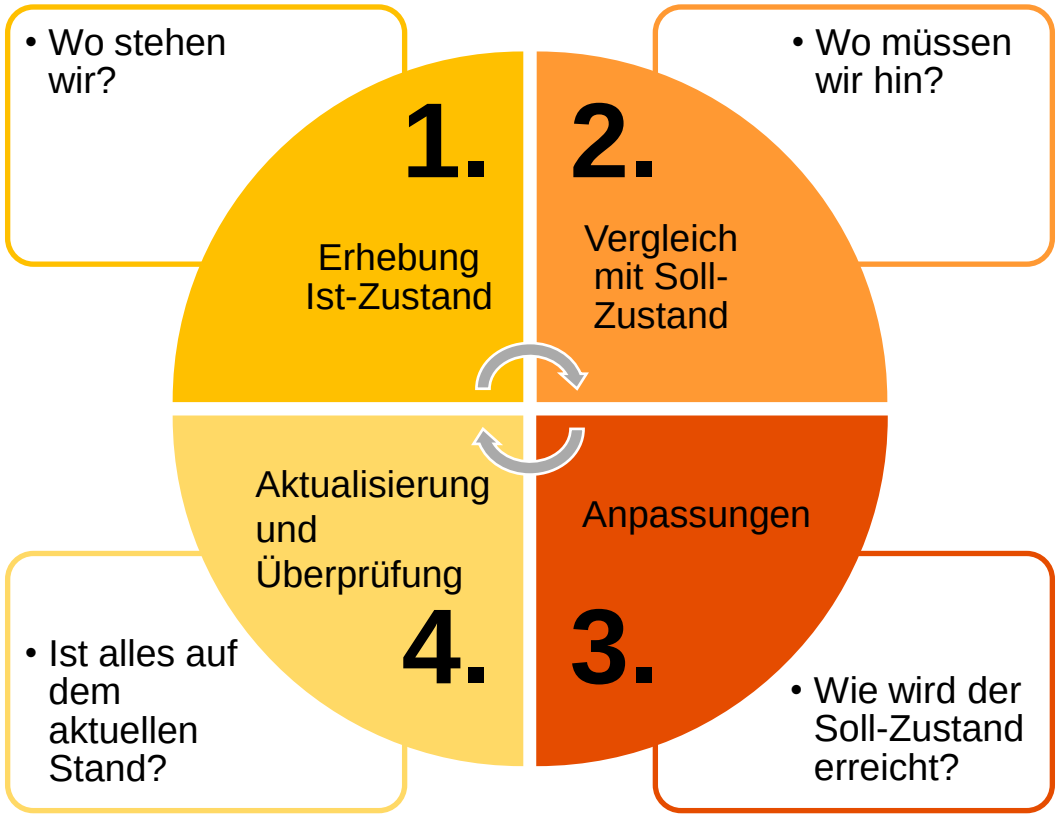
- Gesamtüberblick über den Datenschutz in der Einrichtung gewinnen
  - Wo werden welche Dokumente, wie aufbewahrt?

Vorschlag einer Ordnerstruktur:



III. Umsetzung in der Praxis

Arbeiten mit dem Datenschutzkonzept



IV. Beispiele

Arbeiten mit dem Datenschutzkonzept

Beispiel 1: Verzeichnis von Verarbeitungstätigkeiten (VVT)

Worum geht es?

Soll-Zustand

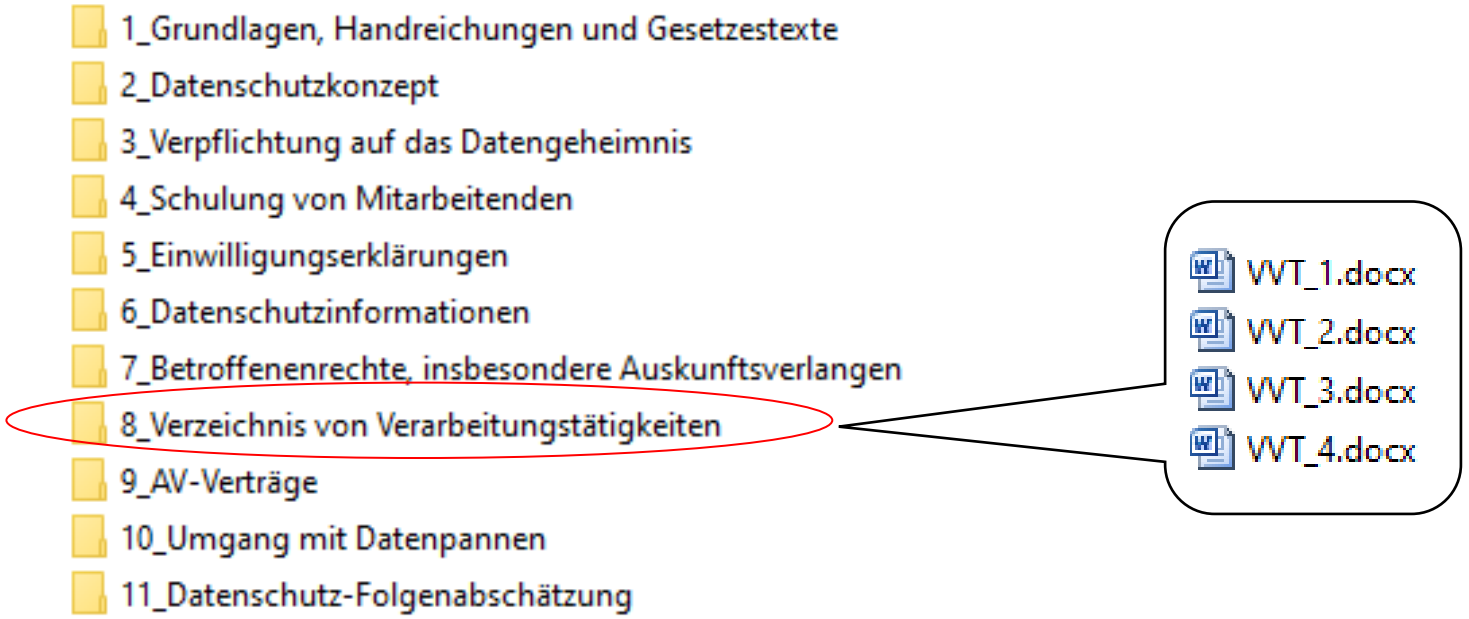
Thema	Referenzvorgaben bzw. Empfehlungen der Stabsstelle Datenschutz	Ist-Zustand	To-do
Erstellung von VVT	Der Verantwortliche hat nach § 31 Abs. 1 KDG ein Verzeichnis von Verarbeitungstätigkeiten (VVT) zu führen, die seiner Zuständigkeit unterliegen. Das VVT muss die in § 31 Abs. 1 KDG genannten Angaben enthalten. Vorlagen, eine Handreichungen und diverse Muster für VVT's finden Sie hier.[5]		
Aktualisierung	Gem. § 1 Abs. 5 KDG-DVO ist das Verzeichnis bei jeder Veränderung eines Verfahrens zu aktualisieren. Im Übrigen ist es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen zu unterziehen und bei Bedarf zu aktualisieren. Die Überprüfung ist in geeigneter Weise zu dokumentieren.		
Aufbewahrung	Das VVT ist in Papierform abzulegen und/oder in elektronischer Form zu speichern, § 31 Abs. 3 KDG.		

Aktueller Ist-Zustand in der Einrichtung

Was muss getan werden, um den Soll-Zustand zu erreichen?

IV. Beispiele

1. Ordner „Verzeichnis von Verarbeitungstätigkeiten“ im Dateisystem öffnen



IV. Beispiele

1. Ordner „Verzeichnis von Verarbeitungstätigkeiten“ im Dateisystem aufrufen
2. Datenschutzkonzept öffnen
3. Erheben Sie den Ist-Zustand für das jeweilige Thema
4. Stellen Sie Abweichungen zum Soll-Zustand fest, dokumentieren Sie dies.

Thema	Referenzvorgaben bzw. Empfehlungen der Stabsstelle Datenschutz	Ist-Zustand	To-do
Erstellung von VVT	Der Verantwortliche hat nach § 31 Abs. 1 KDG ein Verzeichnis von Verarbeitungstätigkeiten (VVT) zu führen, die seiner Zuständigkeit unterliegen. Das VVT muss die in § 31 Abs. 1 KDG genannten Angaben enthalten. Vorlagen, eine Handreichungen und diverse Muster für VVT’s finden Sie hier.	Aktuelle Version des VVT: VVT Version: 2 v. 05.05.2021 Anhang VVT. C TOM momentan in der Erstellung.	VVT. C TOM mit IT-Partner erstellen

IV. Beispiele

Thema	Referenzvorgaben bzw. Empfehlungen der Stabsstelle Datenschutz	Ist-Zustand	To-do
Aktualisierung	Gem. § 1 Abs. 5 KDG-DVO ist das Verzeichnis bei jeder Veränderung eines Verfahrens zu aktualisieren. Im Übrigen ist es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen zu unterziehen und bei Bedarf zu aktualisieren. Die Überprüfung ist in geeigneter Weise zu dokumentieren.	VVT wurde zuletzt am „Datum“ durch den Verantwortlichen überprüft.	Einführung einer neuen Software in VVT aufnehmen und als neue Version VVT_3 speichern. Nächste Überprüfung am: - > Januar 2023

IV. Beispiele

Thema	Referenzvorgaben bzw. Empfehlungen der Stabsstelle Datenschutz	Ist-Zustand	To-do
Aufbewahrung	Das VVT ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann, § 31 Abs. 3 KDG.	VVT befindet sich in elektronsicher Form im Dateisystem im Ordner „Verzeichnis von Verarbeitungstätigkeiten“. und Teile des VVT befinden sich in Papierform in einer Handakte.	Ziel: Einheitliches System: herstellen -> Papierformate digitalisieren

IV. Beispiele

Beispiel 2: Betroffenenrechte, §§ 17 – 25 KDG

Fragestellung/Kontrollfragen	To-do/Notizen
Wer bearbeitet eingehende Anfragen? 1. Innerhalb der Einrichtung ist geregelt, wer Anfragen zu Betroffenenrechten bearbeitet. (Die Festlegung von Zuständigkeiten können unter 3. Zuständigkeitsregelungen dokumentiert werden.)	Für die Bearbeitung von Anfragen nach § 17 KDG ist zuständig:
2. Vertretungsregelungen, z.B. bei Urlaub oder Krankheit sind getroffen.	Die Vertretung übernimmt:
Wie werden die Anfragen bearbeitet? 1. Innerhalb der Einrichtung ist geregelt, wie die Bearbeitung von Anfragen abläuft. 2. Das Verfahren wird **dokumentiert**.	Eine Checkliste für das Auskunftsverlangen nach § 17 KDG finden Sie hier.

IV. Beispiele

Beispiel 3: Dokumentation der IT-Systeme

Thema	Referenzvorgaben bzw. Empfehlungen der Stabsstelle Datenschutz	Ist-Zustand	To-do
Dokumentation der IT-Systeme	Alle in der kirchlichen Einrichtung vorhandenen IT-Systeme und Softwarekomponenten sollten in einem Bestandsverzeichnis, o. ä. aufgelistet sein. Dies ermöglicht u. a. auch ein schnelles Handeln beim Ausfall einzelner Komponenten. Beispiele: Führen von Systemplänen, Hardware-Listen, Netzwerkplänen etc.	Angeschlossen an das diözesane Intranet durch einen offiziellen IT-Partner. Der IT-Partner erstellt die entsprechenden Dokumentationen im Rahmen des drsStandards.	Bei Neuanschaffungen sind die Dokumentationen durch den IT-Partner zu aktualisieren.

IV. Beispiele

Beispiel 4: Dokumentation der IT-Sicherheit

Maßnahme		Ist-Zustand	To-do
Technische Maßnahme	Beispiele: • Benutzerkennung (Identifikation) + Kennwort (Authentisierung) • Sperrung des Zugangs zu dem IT-System bei mehrmaliger Falscheingabe • Erstellung von Benutzerprofilen	Noch keine Zugangsberechtig-ungen zum internen Netzwerk auf Grundlage eines Berechtigungs-konzeptes festgelegt.	Berechtigungskonzept mit IT-Partner erstellen und regelmäßig überprüfen. Nächster Termin: XX.XX.2022
Organisatorische Maßnahme	Beispiele: • Verwendung von starken Passwörtern und Veröffentlichung einer Richtlinie • Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen • Zwei-Faktor-Authentifizierung	Beschäftigte werden regelmäßig von ihrer Führungskraft auf den sicheren Umgang mit Passwörtern hingewiesen.	Gegebenenfalls aktuelle Empfehlungen des BSI-Standards beachten.

V. Zusammenfassung

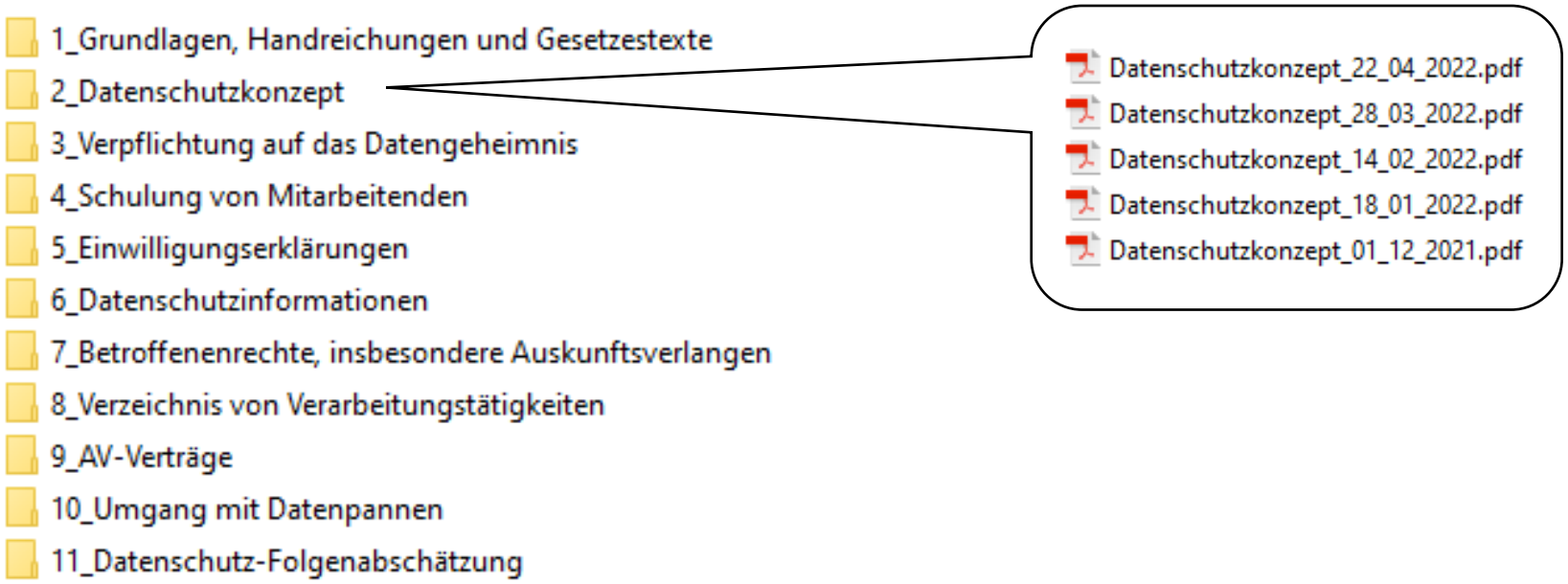
Aktualisierung und Überprüfung

Das Datenschutzkonzept sollte immer auf dem aktuellsten Stand sein.

- regelmäßige Aktualisierung
  - bei jeder Veränderung (siehe Beispiel VVT, Zuständigkeiten, Abläufe, Regelungen etc.)
- regelmäßige Überprüfung
  - Prüfintervall maximal 2 Jahre (§ 7 Abs. 1 S. 1 KDG-DVO)

V. Zusammenfassung

Dokumentation der verschiedenen Versionen



Neue Version des Datenschutzkonzepts wird mit aktuellem Datum abgespeichert.

- Alte Version nicht überschreiben.
- Es muss nachvollziehbar sein, **wer** im Dokument **wann** etwas geändert hat.

V. Zusammenfassung

Zusammenfassung

1. Legen Sie den Geltungsbereich für das Datenschutzkonzept fest.
2. Benennen Sie Ansprechpartner und legen Sie die Zuständigkeiten für den Datenschutz in Ihre Einrichtung fest.
3. Implementieren Sie ein Dateisystem (Ordner-Struktur) in Ihrer Einrichtung.
4. Erheben Sie den Ist-Zustand und passen Sie diesen ggf. an den Soll-Zustand an.
5. Aktualisieren und überprüfen Sie den Ist-Zustand regelmäßig.
6. Bei Rückfragen sprechen Sie bitte die Stabsstelle Datenschutz an.