VA Durchführung einer Bestandsaufnahme der IT-Infrastruktur zur Umsetzung der rechtlichen Rahmenbedingungen

Übersicht

Diese VA dient der internen Unterstützung der Verantwortlichen in der rechtskonformen Umsetzung der IT-Sicherheits- und Datenschutz-Rahmenbedingungen

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zur Durchführung Bestandsaufnahme der technischen und organisatorischen Infrastruktur in geregelten Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung der Vollständigkeit und Qualität der Bestandsaufnahme.

Anwendungsbereich

Diese Anweisung gilt für alle Anwendungen in betrieblichen Prozessen mit Einsatz von Informationstechnik inklusive mobiler Endgeräte wie Smartphones, Tablet-Computer und Laptops.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Einrichtungsleitung/Mitglieder der Leitung (operativ und organisatorisch)
- IT-Sicherheitsbeauftragte (ISB) und IT-Sicherheitskoordinatoren (ISK)
- Externe Dienstleister, soweit rechtlich (schriftlich) geregelt

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse:

<u>Vorbereitung</u>

Im Rahmen der regelmäßigen Mitarbeiterbesprechungen werden Rollen zur Durchführung der Bestandsaufnahme der technischen und organisatorischen Infrastruktur (TOI) definiert und mit den zuständigen Teammitgliedern abgestimmt. In der Standard-Organisation wird die Bestandsaufnahme durch die / den Datenschutzkoordinator(in) geregelt.

<u>Aufgabenverteilung</u>

Die Bestandsaufnahme umfasst umfangreiche interne und externe Recherchen (IT-Partner/DLO) und muss deshalb im Regelfall auf unterschiedliche Personen/Rollen verteilt werden.
Bei größeren Kircheneinrichtungen empfiehlt sich die Erstellung eines strukturierten Projektplans, um die Transparenz der Aufgaben zu gewährleisten.

Einzelprozesse

Eingesetzte IT-Produkte allgemein

- Welche IT-Systeme werden zur Erfassung und Speicherung persönlicher Daten eingesetzt?
- Wie wird die sichere Verknüpfung zwischen verschiedenen IT-Systemen und Spezialdatenerfassung sichergestellt (z.B. Daten in operativen und administrativen Systemen)?

Eingesetzte Hardware (Endgeräte)

- Welche Hardware wird für die Datenspeicherung eingesetzt?
- Welche Hardware wird für die Spezialdatenerfassung verwendet?
- Welche zusätzliche Hardware wird zur Dateneingabe eingesetzt (Scanner, IoT)?

Datensicherung

- Operative Anwendungen (Auftragsverwaltung)
- Administrative Anwendungen (Buchhaltung)

Ausgabe von personenbezogenen Daten

Ausgabe aus der Personalkartei

- An Angehörige
- An Kooperationspartner
- An Auftragsverarbeiter
- An offizielle Stellen

Datenfernkommunikation (z.B. Fernwartung) hier: Datenkategorien

Kontaktdatenverwaltung ISMS/DSMS relevant (separate Dokumentation: siehe VA)

Ergebnis

Das Ergebnis der Bestandsaufnahme wird in das Dokument „Bestandsaufnahme zur Infrastruktur“ aufgenommen.

Wartung und Aktualisierung

Mindestens einmal jährlich wird die Bestandsaufnahme für den Jahresbericht aktualisiert.

Bei wesentlichen Veränderungen erfolgt ebenfalls eine Aktualisierung:

- Einsatz neuer Server HW
- Erweiterung des IT-Netzwerks
- Anschluss neuer Peripherie
- Erweiterung oder Wechsel der Software
- Erweiterung oder Ersteinsatz von Zusatz-SW (z.B. Studien/Q-Register)
- Neue Anwendungen Datenfernkommunikation (z.B. Telematikinfrastruktur/TI)

Anschließend wird die Risikoanalyse erneuert, um die anschließende Datenschutz-Folgeabschätzung (DSFA) ebenfalls zu aktualisieren.

Aktualisierung: nach 12 Monaten

Mitgeltende Dokumente:

- Datenschutz-Regelungen der Evangelischen Kirche
- Cyberschutz-Regelungen der Evangelischen Kirche