Anlage 8

**Einbezug der Mitarbeitervertretung**

(Stand: Beschlussfassung im Kreiskirchenrat KKSOL, 15. Oktober 2019)

Grundsätze:

Im vorliegenden IT-Sicherheitskonzept geht es sowohl um IT-Sicherheit als auch um Datenschutz.

Fortbildungen für alle IT-Nutzer zu Thema IT-Sicherheit und Datenschutz sind unbedingt not-wendig. Das Angebot dafür ist allen zugängig zu machen und eine Teilnahme zu ermöglichen.

Per Gesetz besteht bei Aufnahme einer Tätigkeit die Verpflichtung, die anzustellende Person auf das Datengeheimnis zu verpflichten (§ 26 DSG-EKD, § 7 DSGVO). Dies ist gleichzusetzen mit der Verschwiegenheitserklärung die ggf., bereits unterschrieben wurde,

[offene Aufgabe: im Konsistorium ist zu prüfen, ob nicht beide Vorlagen zusammenzubringen sind.]

IT-Einrichtung und deren Betrieb, sowie organisatorische Regelungen erfolgen unter Beachtung des geltenden Datenschutzrechts in besonderer Anerkennung des Grundrechts auf in-formationelle Selbstbestimmung.

Aufgaben im Rahmen des IT-Sicherheitskonzeptes und weitere Hinweise:

Es ist ein Rollen-Konzept zu erstellen, nach welchen Bereichen Zugriffsrechte voneinander abgegrenzt und zugewiesen werden. Dabei sind folgende drei Ebenen zu unterscheiden:

* IT-Nutzende (privat bzw. öffentlich-rechtlich angestellte Beschäftigte)
* AdministratorInnen
* IT-Sicherheits-Beauftragte

In der Dienstanweisung (Anlage 4) sind die Beschäftigten darauf hinzuweisen, sofort eine Gefährdungsanzeige herzustellen, wenn technische, organisatorische und andere geforderte Maßnahmen wegen fehlender Verfügbarkeiten oder Voraussetzungen für die Mitarbeitenden nicht ausführbar sind

Beteiligung der Mitarbeitervertretung

Alle Maßnahmen, die der Mitbestimmung unterliegen, sind der Mitarbeitervertretung nach Maßgabe des Mitarbeitervertretungsrechts rechtzeitig, umfassend und in angemessener Form mitzuteilen. Die Informationen müssen so erfolgen, dass die Mitarbeitervertretungen ihre Mitwirkungs- und Mitbestimmungsrechte effektiv wahrnehmen können. Die Informationen müssen die möglichen mitarbeitervertretungsrechtlichen Folgen ersichtlich und beurteilbar machen.

Das betrifft insbesondere folgende Bereiche des IT-Sicherheitskonzeptes in Anlage 4:

* **Anlage 4, Teil A, Nr. 3. d.** – die dienstliche bzw. private Nutzung und Überwachung unterliegt der Mitbestimmung
* **Anlage 4, Teil A, Nr. 3. f.** – die Einführung von Software unterliegt der Mitbestimmung, wenn sie geeignet ist Verhalten und Leistung zu kontrollieren und zu überwachen.
* **Anlage 4, Teil A, Nr. 3. j.** – unterliegt der Mitbestimmung.

- **Anlage 4, Teil A, Nr. 4** – Regelungen zu Ordnung und Verhalten unterliegen der Mitbestimmung

- **Anlage 4, Teil A, Nr. 7. d.** – hier ist zu klären, ob es besser ist, die Aufgabe der Administratorin bzw. dem Administrator mit betrieblichem Datenschutzbeauftragten und der MAV zu übertragen.

* **Anlage 4, Teil A, Nr. 8** – die MAV hat der vorliegenden Fassung zugestimmt

Kontinuierliche Klärungen in Bezug auf das IT-Sicherheitskonzept:

Es ist kontinuierlich zu klären und zu prüfen, ob für alle Regelungen auch immer alle Voraussetzungen geschaffen sind.

Es ist kontinuierlich zu klären und zu prüfen, ob die installierte und verwendete Software den Anforderungen des IT-Sicherheitskonzeptes entspricht.

Die Voraussetzungen Anlage 4, Teil B, Nr. e., vertrauliche oder personengebundene Daten auf mobilen Datenträgern immer verschlüsselt zu speichern. sind zu schaffen und bereitzu-stellen.

Es ist zu keinem Zeitpunkt gestattet, eine automatische Weiterleitung von elektronischen Nachrichten, wie etwa E-Mails, an Dritte vorzunehmen. Abwesenheiten können durch einen Abwesenheitsassistenten bekannt gegeben werden.

Ausdrücklich ist noch einmal darauf hinzuweisen, dass der Zugriff auf ein personenbezogenes Postfach durch andere Personen als die entsprechend berechtigten Mitarbeitenden grundsätzlich nicht erlaubt ist.

Es ist möglich, die Datenschutzangelegenheiten einer Kirchengemeinde an die Datenschutz-beauftragten auf Kirchenkreisebene zu delegieren.