Konzept
zum Datenschutz und zur Datensicherheit
bei der elektronischen Weitergabe von Unterlagen
an die Mitglieder kirchlicher Gremien

Einleitung

Viele kirchliche Gremien sind dadurch gekennzeichnet, dass sie in großer Zahl (häufig sogar mehrheitlich) aus ehrenamtlichen Mitgliedern bestehen, bei denen die Datenverarbeitung auf privaten Endgeräten erfolgt.

Es ist kaum möglich, die privaten Endgeräte ehrenamtlich tätiger Personen durch technische und organisatorische Maßnahmen in gleicher Weise gegen unbefugten Zugriff zu schützen wie dienstliche Geräte. Dennoch muss gewährleistet sein, dass bei Unterlagen mit hohem Schutzbedarf, die den Mitgliedern kirchlicher Gremien zur Verfügung gestellt werden, auch in dieser Konstellation insbesondere die Integrität und die Vertraulichkeit der Daten gewahrt bleiben.

Begriffsbestimmungen

- **„Personenbezogene Daten“** sind gemäß § 4 Absatz 1 DSG-EKD alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Diese Definition ist EKD-weit geltendes Recht. Der genaue Inhalt ist im Einzelfall insbesondere durch systematische Auslegung des ganzen DSG-EKD zu ermitteln.

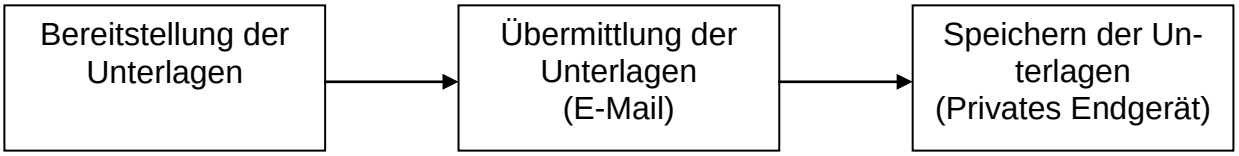
- „**Besonders schützenswert**“ sind alle Unterlagen, deren Kenntnisnahme durch Unbefugte der jeweiligen kirchlichen Stelle oder der Landeskirche insgesamt Schaden zufügen könnte.

Datenschutz und -sicherheit bei der elektronischen Weitergabe von Unterlagen an die Mitglieder kirchlicher Gremien

Bei der elektronischen Weitergabe von Unterlagen an die Mitglieder kirchlicher Gremien sind drei Phasen zu unterscheiden:

1. Die Bereitstellung der Unterlagen
2. Die Übermittlung der Unterlagen (in der Regel per E-Mail)

3. Das Speichern der Unterlagen auf dem privaten Endgerät



Das vorliegende Konzept legt den Schwerpunkt nicht auf die Absicherung des Endgeräts, sondern darauf, schon in der Phase 1 den Schutzbedarf der Unterlagen festzulegen und danach die Form, in der die Dateien bereitgestellt werden (verschlüsselt oder unverschlüsselt), zu bestimmen.

Das Konzept im Detail:

1. Phase: Bereitstellung der Unterlagen

   Schon beim Erstellen der Unterlagen für das kirchliche Gremium legt die dafür zuständige Person den Schutzbedarf fest und vermerkt dies auf dem Deckblatt der Unterlage.

   Hohem Schutzbedarf unterliegen alle Unterlagen mit personenbezogenem Inhalt sowie alle Unterlagen, die nach obiger Definition „besonders schützenswert“ sind.

   Alle anderen Unterlagen unterliegen dem normalen Schutz. Das kirchliche Gremium hat die Möglichkeit, die Schutzklasse einer Unterlage in seiner Sitzung zu ändern.

   Im Büro des jeweiligen kirchlichen Gremiums werden alle Unterlagen, für die ein hoher Schutzbedarf festgestellt worden ist, vor dem Versand in PDF-Dateien umgewandelt und verschlüsselt. Der Schlüssel wird den Mitgliedern des kirchlichen Gremiums auf gesondertem Wege (nicht per E-Mail) mitgeteilt. Er bleibt für zwölf Monate gültig und wird in der Regel innerhalb dieses Zeitraums nicht geändert.

2. Phase: Übermittlung der Unterlagen

   Alle Mitglieder des kirchlichen Gremiums, auch die ehrenamtlichen, erhalten für die Zeit, in der sie ihr Amt bekleiden, eine dienstliche E-Mail-Adresse (z. B. vorname.nachname@kirchliche_stelle.de). Das Büro des jeweiligen kirchlichen Gremiums versendet die Unterlagen als E-Mail-Anhang ausschließlich an diese Adressen. Damit ist gewährleistet, dass alle Unterlagen in einem geschützten Netz übertragen werden.

   Damit diese E-Mails den geschützten Bereich nicht verlassen, muss eine Weiterleitung an private E-Mail-Adressen unterbleiben.

Alternativ dazu besteht auch die Möglichkeit, die Unterlagen auf einer Intranet-Plattform zum Download bereitzustellen. Die Mitglieder des kirchlichen Gremiums erhalten eine passwortgeschützte Zugangsberechtigung und damit die Möglichkeit, die Unterlagen über eine gesicherte Verbindung abzurufen.

3. Phase: Speichern der Unterlagen auf dem privaten Endgerät

Alle Mitglieder des kirchlichen Gremiums erhalten Hinweise zum Schutz ihrer privaten Endgeräte gegen unbefugten Zugriff. Diese Hinweise gehen aber nicht über das hinaus, was jede Privatperson ohnehin zum Schutz ihrer Daten tun sollte. Ein erhöhter Aufwand ist nicht erforderlich, da die besonders schützenswerten Unterlagen von vornherein nur in verschlüsselter Form vorliegen.

Folgende Sicherheitsmaßnahmen sollten auf den privaten Endgeräten getroffen werden:

- Passwortschutz
- Virenschutz
- Firewall
- Regelmäßige Sicherheitsupdates

Das Verschlüsseln der Festplatte bzw. eines Teils davon zum Speichern der Unterlagen wird zwar empfohlen, ist aber nicht zwingend.

Der Passwortschutz der mit Passwort versendeten Dateien darf nicht umgangen werden und muss beim Speichern auf den Endgeräten erhalten bleiben.