



EDV Persönlichkeits- und Datenschutz

1 Grundlagen

1.1 EDV Netzwerk

Die Kirchgemeinde betreibt ein eignes EDV Netzwerk bestehend aus einem Server und den entsprechenden Arbeitsstationen. Dem Schutz der Daten, insbesondere der vertraulichen seelsorgerischen Daten, wird höchste Priorität beigemessen. Das Netzwerk ist nach modernsten Gesichtspunkten aufgebaut und erfüllt alle gängigen Sicherheitsstandards.

1.2 EDV Administration

Die Administration der EDV Anlagen und Netzwerke wird durch eine professionelle Firma gewährleistet. Diese externe Firma ist den standesüblichen Vorschriften betreffend EDV Datenschutz verpflichtet. Drittpersonen haben keinen Zugang zum EDV Netzwerk und somit zu keinen Daten.

2 EDV Datenschutz in der Kirchgemeinde Datensicherung

2.1 Persönlicher Zugangscode (Login/Passwort)

Jeder Mitarbeiter der Kirchgemeinde hat einen persönlichen Zugangscode zum Netzwerk. Mit diesem Zugangscode (Login und Passwort) kann er an einem beliebigen Arbeitsplatz auf die persönliche Daten zugreifen. Das Passwort kann jeder Mitarbeiter selbständig ändern. Es wird auf die Sorgfaltsmassnahmen bei der Auswahl einen neuen eigenen Passwortes hingewiesen.

2.2 Persönliche Daten

Die persönlichen Daten sind geschützt und können von Drittpersonen nicht eingesehen werden. Achtung, alle Daten die via E-Mail versandt werden sind grundsätzlich nicht geschützt. E-Mails werden von externen Organisationen überwacht.

Die Kirchgemeinde erlaubt den Zugriff auf das Internet und „Soziale Netzwerke“. Daten in „Sozialen Netzwerken“ sind grundsätzlich nicht geschützt. Die Kirchgemeinde ist für den Missbrauch von Daten, die Mitarbeiter im Internet preisgeben nicht haftbar.

2.3 Datensicherung

Die Kirchgemeinde sichert alle Daten und E-Mails. Die Datensicherung erfolgt mit modernen Methoden. Die Sicherungskopien können von Dritten nicht eingesehen werden. Zur Aufklärung von Verbrechen kann die Kirchgemeinde gezwungen werden die Daten an die entsprechenden Behörden auszuliefern.

2.4 Administration

Der „Administrator“ hat Zugriff auf alle Daten auf dem Server. Die individuellen Benutzerdaten sind jedoch im Normalfall geschützt. Der Administrator kennt die Zugangscodes der Benutzer nicht. In Falle eines Verbrechens kann der Administrator die Zugangscodes jedoch sperren. Nach einem Totalausfall des Servers müssen alle Zugangscodes neu erstellt werden.

Der Administrator unterliegt der Schweigepflicht. Er darf unter keinen Umständen auf geschützte Daten zugreifen ohne Erlaubnis des entsprechenden Benützers. Die Weitergabe von Daten an Dritte ist strengstens verboten.



2.5 Remote Support

Die allgemeine Software Wartung wird auf allen System und Arbeitsplätzen regelmässig durchgeführt und beeinträchtigen die Benutzer nicht. Auf Wunsch wird „Remote Support“ geleistet, d.h. der Administrator verbindet sich von seinem Arbeitsplatz direkt auf den Arbeitsplatz des Benützers. Damit kann der Administrator sehen was das Problem des Benützers ist und dem Benutzer direkt und unkompliziert helfen.

Remote Support wird nur auf ausdrücklichen Wunsch des Benützers geleistet. Der Benutzer muss sein Einverständnis geben bevor der Administrator sich auf seinen Arbeitsplatz verbindet. Nach Abschluss der Arbeiten löst der Administrator die Verbindung wieder und informiert den Benutzer entsprechend. Der Administrator hat kein Recht sich unaufgefordert oder ohne Wissen des Benützers auf den Arbeitsplatz zu verbinden.

Goldach, 13. April 2010

Im Namen der Verwaltung
Der Präsident: Ruedi H. Egger
Der Verwalter: Daniel Gerster