

# Technisches Sicherheits- und Datenschutzkonzept [www.ekful.net](http://www.ekful.net)

Stand: 06. August 2008

## 1 Vertraulichkeit, Anonymität und Datenlöschung

### 1.1 Vertraulichkeit

Ziel des Systems zur Webmail-Beratung ist es, in der Online-Kommunikation einen Grad der Vertraulichkeit herzustellen, der mit einem Vier-Augen-Gespräch innerhalb einer Beratungsstelle vergleichbar ist.

Auf technischem Wege wird dabei sicher gestellt, dass Beratungsanfragen nach der Fallverteilung nur von dem/der Ratsuchenden und einem/einer Berater/in gelesen werden können. Ein Mitlesen von Beratungsinhalten durch Dritte („Monitoring“ / „Intervision“) ist technisch nicht vorgesehen.

Supervision sollte lokal im Team der örtlichen Beratungsstelle gegebenenfalls mit Ausdrucken auf Papier stattfinden.

### 1.2 Anonymität

- Ratsuchende brauchen ihren Namen nicht anzugeben, es wird lediglich eine zufällige Anfragenummer zur Identifizierung des/der Ratsuchenden vergeben.
- Ratsuchende können freiwillig eine E-Mail-Adresse angeben, an die sie automatisierte Benachrichtigungen erhalten, sobald eine Antwort auf Ihre Anfrage vorliegt.
- Berater/innen können die E-Mail-Adressen von Ratsuchenden nicht sehen. Es werden niemals Beratungsinhalte oder persönliche Daten per E-Mail versendet.
- Die IP-Adresse von Ratsuchenden wird nicht zusammen mit der Anfrage gespeichert.
- Es werden keine Benutzerprofile angelegt, die es ermöglichen, eine Verbindung zwischen verschiedenen Anfragen herzustellen.

### 1.3 Datenlöschung

Alle Nachrichten werden zeitnah nach Beendigung einer Anfrage gelöscht. Die Löschung erfolgt automatisch wenn innerhalb von 60 Tagen keine neue Nachricht ausgetauscht wurde. Nachrichten werden zudem unmittelbar gelöscht, wenn Ratsuchende ihre Anfrage selbst beenden.

Durch die „Schutzfrist“ von 60 Tagen ist gewährleistet, dass eine Anfrage auch dann fortgesetzt werden kann, wenn sie durch Urlaub oder Krankheit des/der Berater/in oder des/der Ratsuchenden einige Wochen unterbrochen wird.

Eventuelle Dokumentations- und Archivierungspflichten verbleiben bei der Beratungsstelle. Hierzu ist es möglich, Nachrichten auszudrucken.

## **2 Übertragungssicherheit**

### **2.1 SSL-Verschlüsselung**

Die Datenübertragung erfolgt ausschließlich über eine SSL-verschlüsselte Verbindung. Unverschlüsselte Verbindungen werden serverseitig nicht zugelassen.

Unverschlüsselte E-Mails werden optional zur Benachrichtigung über den Eingang neuer Nachrichten verwendet. Sie enthalten jedoch keine personenbezogenen Daten.

### **2.2 Authentifizierung**

Der Zugriff auf geschützte Beratungsinhalte ist ausschließlich für authentifizierte Nutzer/innen zugelassen. Hierzu wird eine Session-Id per Cookie übergeben. Es werden dabei nicht-persistente Cookies eingesetzt, die nach Schließen des Browsers automatisch gelöscht werden.

### **2.3 Schutz vor sogenannten Brute-Force-Angriffen**

Nach 10 erfolglosen Anmelde-Versuchen auf einem Benutzerkonto wird das betreffende Konto für 24 Stunden gesperrt. Dadurch soll verhindert werden, dass unberechtigte Personen durch wahlloses Ausprobieren von Passwörtern Zugang zum System erhalten.

## **3 Serverseitige Sicherheit**

### **3.1 Providerauswahl**

Bei der Auswahl des Providers sind die besonderen Bestimmungen von §11 Datenschutzgesetz der EKD zu beachten. Daher erfolgt das Hosting in einem kirchlichen Rechenzentrum.

### **3.2 Verschlüsselung**

Alle Nachrichten, der Anfragebetreff und die E-Mail-Adressen der Ratsuchenden werden verschlüsselt gespeichert. Dabei kommen die folgenden, anerkannten Verfahren zum Einsatz:

- AES-Verschlüsselung mit 256 Bit Schlüssellänge
- RSA-Verschlüsselung mit mindestens 1024 Bit Schlüssellänge

Durch den Einsatz von Verschlüsselung ist sicher gestellt, dass ohne die Kenntnis der Passwörter der jeweils zugriffsberechtigten Personen ein Lesen der Daten nicht möglich ist. Dies gilt auch für Personen mit vollen Systemrechten wie Administratoren/innen.

## **4 Clientseitige Sicherheit**

### **4.1 Qualität der Passworte**

Ratsuchende und Berater/innen wählen ihre Passworte selbst aus. Passworte müssen aus mindestens acht Zeichen bestehen und sowohl Buchstaben als auch Zahlen enthalten.

### **4.2 Schutz vor lokaler Speicherung von Benutzereingaben**

Die lokale Speicherung von Passwörtern und anderen Formulareingaben durch den Browser wird – soweit technisch möglich – unterbunden. Hierbei kommt ein Verfahren zum Einsatz, wie es auch beim Online-Banking Verwendung findet.

### **4.3 Verwendung ausschließlich dienstlicher Computer**

Für die Online-Beratung werden ausschließlich dienstliche Computer in den Räumen der Dienststelle verwendet.

### **4.4 Schutz vor Viren und anderen Schadprogrammen**

Alle beteiligten Beratungsstellen sehen besondere Sicherheitsvorkehrungen zum Schutz der zur Online-Beratung verwendeten Computer vor. Als Orientierung hierfür können die im Folgenden unter A bis C genannten Schutzkonzepte dienen.

#### **A. Professionell administrierte EDV-Infrastruktur**

Die Dienststelle organisiert eine professionell administrierte EDV-Infrastruktur, inklusive Firewall, Virenschutz und gestufter Benutzerverwaltung. Diese Lösung kommt für Beratungsstellen mit Einbindung in eine größere Organisationsstruktur in Frage.

#### **B. Internet-Zugang ausschließlich über externe Firewall**

Verfügt der Träger / die Beratungsstelle nicht über die personellen Ressourcen für den Aufbau einer professionell geschützten Umgebung, kann der Schutz eines kleinen lokalen Netzwerks über eine externe Firewall erfolgen (z.B. kondek.dsl-flat).

#### **C. Nutzung von Thin-Clients**

Eine einfache und kostengünstige Lösung für kleine Beratungsstellen, ist der Einsatz eines so genannten Thin-Client-Computers. Dieser sollte über keine Festplatte und keine Möglichkeit zur Installation weiterer Programme verfügen.

## **5 Datenschutzhinweis**

Die Website enthält einen allgemein verständlichen Datenschutzhinweis für die Benutzer/innen des Systems nach den einschlägigen gesetzlichen Regelungen. Darin soll auch der bzw. die Datenschutzbeauftragte als Ansprechpartner/in genannt werden.