

Gemeinsamer Standard bei Verfahren zur Online-Beratung

Ratsuchende bringen Online-Beratungsangeboten ein erhebliches Maß an Vertrauen dahingehend entgegen, dass dabei die Vertraulichkeit gewahrt bleibt. Die christlichen Kirchen stehen aufgrund ihres seelsorgerischen Auftrags in einer besonderen Pflicht, diese sicher zu stellen.

Eine Enttäuschung dieses Vertrauens kann zudem die weitere Inanspruchnahme solcher Angebote empfindlich beeinträchtigen und zu einem nur schwer behebbaren Imageverlust der hinter den Beratungsangeboten stehenden kirchlichen Stellen und Organisationen führen.

Die nachfolgenden Anforderungen sind von Softwareherstellern, die für kirchliche Stellen Verfahren zur Online-Beratung entwickeln, einzuhalten. Bereits bestehende Verfahren, die nicht alle Anforderungen erfüllen, werden baldmöglichst auf einen entsprechenden Stand gebracht.

1. Ratsuchende oder Beratende greifen auf die Webseiten des Verfahrens ausschließlich im Rahmen einer gesicherten Verbindung (https-Protokoll) zu.
2. Ratsuchende und Beratende müssen sich für eine Sitzung an dem Verfahren mit einem Benutzernamen oder einer vom Verfahren vergebenen Anfragenummer und einem geheimen Passwort anmelden (Zugangsdaten).
3. Soweit für die Dauer einer Sitzung temporär Daten auf dem von einer ratsuchenden oder beratenden Person verwendeten PC gespeichert werden (z.B. sog. Session-Cookies), erfolgt dies verschlüsselt.
4. Das Verfahren speichert alle Daten der Ratsuchenden und Beratenden verschlüsselt auf einem Server ab. Eine Entschlüsselung von Daten findet ausschließlich temporär für die Dauer einer Sitzung einer ratsuchenden oder beratenden Person statt; dabei werden jeweils nur die benötigten Daten entschlüsselt.
5. Die verschlüsselte Speicherung auf dem Server erfolgt mittels asymmetrischer Verschlüsselung dergestalt, dass eine Entschlüsselung nur mit den persönlichen Zugangsdaten (Passworten) der zugriffsberechtigten Personen möglich ist. Die für die Entschlüsselung notwendigen Schlüssel dürfen nicht im Klartext zusammen mit den Daten auf dem Server abgelegt werden.
6. Für Verfahren, die von einer Vielzahl von Stellen eingesetzt werden oder eingesetzt werden sollen, wird die Bestätigung der Sicherheit und Vertraulichkeit durch eine namhafte Institution angestrebt.
7. Das Verfahren wird auf kirchlichen Servern oder bei kommerziellen Providern, deren Qualität und Sicherheit durch ein Zertifikat ausgewiesen ist, gehostet.

30.04.2009
Konferenz der Datenschutzbeauftragten im
Bereich der Katholischen Kirche
Deutschlands (noch zu beschließen)

30.04.2009
Konferenz der Datenschutzbeauftragten der
evangelischen Landeskirchen