Rundschreiben des Landeskirchenamtes an die Kirchenkreise betreffend • Datenschutz bei Inanspruchnahme externer Wartung und Systembetreuung

Vom 11. Dezember 2000 (Az.: A 14-03/01.09)

[1]Die Abhängigkeit von einer funktionierenden Datenverarbeitung wird bei den kirchlichen Stellen immer größer. [2]Obwohl Hardware und Software prinzipiell zuverlässiger und benutzerfreundlicher geworden sind, ist eine kompetente Betreuung, insbesondere im Fehlerfall, allein durch die kirchlichen Stellen nicht mehr immer sicherzustellen. [3]Gründe hierfür sind die zunehmende Systemkomplexität und verteilte Systemarchitekturen. [4]Zum Teil steht auch nicht genügend ausreichend qualifiziertes Personal bei den kirchlichen Stellen zur Verfügung.

[1]Als Folge davon werden Verträge für Wartungsarbeiten und Systembetreuung mit externen Personen und Firmen abgeschlossen, zum Teil auch mit den DV-Firmen, die das eingesetzte Verfahren entwickelt haben. [2]Gefahren und Risiken drohen bei der Wartung und Systembetreuung dadurch, dass

- für die Wartung ein weiterer Zugang zum Rechner geschaffen wird, über den sich Personen mit umfassenden Rechten anmelden können oder der als Zugang für „Hacker“ missbraucht werden kann;
- die kirchliche Stelle die Fernwartung nur begrenzt kontrollieren kann, z. B. welche Person tatsächlich die Wartung vornimmt, welche Daten übertragen werden und welche Sicherungsmaßnahmen beim Auftragnehmer getroffen worden sind;
- das Wartungspersonal auf den gesamten Datenbestand zugreifen kann;
- der Datenverkehr zwischen dem Rechner der DV-Anlage der kirchlichen Stelle und der externen Wartungsfirma abgehört werden kann.

Datenschutzrechtlich sind für die externe Fernwartung und Systembetreuung die Regelungen der Auftragsverarbeitung nach dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)[1] heranzuziehen:

[1]Nach § 11 DSG-EKD[1] ist die beauftragende kirchliche Stelle für die Einhaltung der Vorschriften des Datenschutzes verantwortlich. [2]Die beauftragte externe Wartungs- oder Systembetreuungsfirma ist unter Berücksichtigung der Eignung der von ihr geplanten technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [3]Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und

1 Nr. **850**.

organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. [4]Das beauftragte Unternehmen darf die Daten nur im Rahmen der Weisungen der kirchlichen Stelle verarbeiten oder nutzen. [5]Ist die Wartungs- oder Systembetreuungsfirma der Ansicht, dass eine Weisung der kirchlichen Stelle gegen das kirchliche Datenschutzrecht verstößt, hat sie die kirchliche Stelle unverzüglich darauf hinzuweisen. [6]Sofern die kirchlichen Datenschutzbestimmungen bei der beauftragten Wartungs- oder Systembetreuungsfirma keine Anwendung finden, ist die kirchliche Stelle verpflichtet, sicherzustellen, dass die beauftragte Stelle diese Bestimmungen beachtet und sich der Kontrolle des kirchlichen Datenschutzbeauftragten unterwirft. [7]In einem Wartungs- bzw. Systembetreuungsvertrag sind die einzuhaltenden notwendigen technischen und organisatorischen Maßnahmen schriftlich festzulegen.

[1]Als **Anlage 1** haben wir ein Merkblatt zu den erforderlichen Sicherheitsmaßnahmen bei der Inanspruchnahme von externem Wartungs- und Systembetreuungspersonal beigefügt. [2]Wir bitten zu beachten, dass sich Art und Umfang der notwendigen Sicherungsmaßnahmen nach der Sensibilität der verarbeiteten Daten und nach der technischen Anbindung richten. [3]Nur die Gesamtheit der notwendigen technischen und organisatorischen Maßnahmen bietet einen ausreichenden Schutz.

[1]Auf Basis des Merkblattes haben wir als **Anlage 2** eine Checkliste zur praktischen Umsetzung des technisch-organisatorischen Datenschutzes beigefügt. [2]Mit der Checkliste haben Sie eine übersichtliche Aufstellung über die bereits getroffenen und noch zu treffenden Maßnahmen.

[1]Eine beantwortete Checkliste kann vorhandene Sicherheitslücken aufzeigen. [2]Daher sollte die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich behandelt werden.

Als **Anlage 3** fügen wir „Empfehlungen zur datenschutzrechtlichen Gestaltung von Fernwartungsverträgen“ bei, die bei Neuabschluss bzw. bei Verlängerung von bestehenden Fernwartungsverträgen zu beachten sind.

Wir schlagen vor, dieses Schreiben einschließlich der Anlagen an alle kirchlichen Stellen weiterzuleiten, die nach Ihrem Kenntnisstand regelmäßig oder gelegentlich auf externe Wartungshilfe oder Systembetreuung zugehen.

Anlage 1

Datenschutz bei externer Wartung und Systembetreuung

Merkblatt der Evangelischen Kirche von Westfalen zum Datenschutz und zur Datensicherheit bei der Inanspruchnahme von externem Wartungs- und Systembetreuungspersonal

– Stand 01.12.2000 –

[1]Auf Grundlage des Schreibens der EKvW vom 11.12.2000, Az.: A 14 – 03/01.09, bietet dieses Merkblatt konkrete Handlungsempfehlungen für technische und organisatorische Sicherungsmaßnahmen. [2]Damit sollen Personen, die mit der Leitung, Fachbereichsleitung, Systembetreuung, der Organisations- oder DV-Leitung betraut sind oder als Ansprechpartnerinnen und Ansprechpartner für Datenschutzfragen bzw. als Betriebsbeauftragte für den Datenschutz berufen worden sind, in die Lage versetzt werden, ein Konzept für eine datenschutzgerechte Wartung und Systembetreuung durch externe Personen oder Firmen zu entwickeln bzw. bestehende Lösungen zu überprüfen.

[1]Die Wartung beinhaltet die Summe der Maßnahmen, die zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von DV-Anlagen notwendig sind. [2]Dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware.

Die externe Wartung (Fernwartung) und Systembetreuung umfasst die Wartung der Hard- und Software von DV-Anlagen durch direkten Eingriff vor Ort in das System und von außerhalb durch Einrichtungen zur Datenübertragung.

Nach § 9 DSG-EKD[1] haben kirchliche Stellen die technischen und organisatorischen Sicherheitsmaßnahmen zu treffen.

1. Maßnahmen zur Zugangskontrolle

1.1. [1]Bei der Wartung und Fernwartung dürfen die Wartungsarbeiten nur auf Anforderung der kirchlichen Stelle begonnen werden. [2]Beginn und Ende der Wartungsarbeiten sollten nach Absprache erfolgen.

1.2. [1]Bei der Wartung von Programmen und Dateien mit sensiblen personenbezogenen Daten ist der Kreis des autorisierten Wartungspersonals vorher festzulegen; ohne genaue Identifikation dürfen keine Wartungsarbeiten beginnen. [2]Bei einer Wartung und Systembetreuung vor Ort hat sich das Wartungspersonal vor Beginn der Arbeiten auszuweisen.

---

1 Nr. **850**.

1.3. Um im Rahmen der Fernwartung zu verhindern, dass unbefugte Personen Zugriff auf das DV-System erhalten, ist der Verbindungsaufbau durch das DV-System der kirchlichen Stelle herzustellen.

1.4. Der Dialog mit der Fernwartungszentrale ist zu unterbrechen, wenn die Verbindung zur Fernwartungszentrale gestört ist („Zwangslogout“) oder erkennbar wird, dass eine missbräuchliche Nutzung erfolgt.

1.5. [1]Die dem Wartungspersonal eingeräumten Zutritts- und Zugangsrechte sind auf das notwendige Minimum zu beschränken. [2]Bei der Wartung und Betreuung von Programmen und Dateien mit sensiblen personenbezogenen Daten sind die Zutritts- und Zugangsrechte nach Abschluss der Arbeiten zu widerrufen bzw. zu sperren.

2. Organisation der Datenträgerkontrolle

2.1. [1]Bevor ein Datenträger mit personenbezogenen Daten den DV-Bereich zu Wartungszwecken oder zur Fehleranalyse verlässt, ist zu prüfen, ob die personenbezogenen Daten für diesen Zweck tatsächlich benötigt werden. [2]Ggf. sind die personenbezogenen Daten zu anonymisieren[1] oder pseudonymisieren[2] bzw. ganz oder teilweise zu löschen. [3]Es sind Nachweise über den Versand zu führen (Begleitzettel, Versandscheine, Empfangsbestätigung).

2.2. [1]Das Wartungspersonal arbeitet möglichst mit Datenträgern der kirchlichen Stelle. [2]Mitgebrachte Datenträger verbleiben für einen bestimmten Zeitraum bei der kirchlichen Stelle für Kontrollzwecke.

2.3. Bei der Wartung und Betreuung von Programmen und Dateien mit sensiblen personenbezogenen Daten ist darauf zu achten, dass das Wartungspersonal keine am DV-System erzeugten Datenträger ungelöscht mitnehmen kann.

2.4. Alle Wartungs- und Übertragungsaktivitäten müssen i. d. R. am Bildschirm zum Mitlesen sichtbar sein.

3. Maßnahmen zur Speicherkontrolle

3.1. Es wird davon ausgegangen, dass alle Programme mit personenbezogenen Daten durch Passworte geschützt sind.

---

1 Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können.

2 Pseudonymisieren ist das Ersetzen des Namens durch ein drittes nicht bekanntes Identifizierungsmerkmal (Pseudonym).

3.2. [1]Das Wartungspersonal muss sich einer Anmeldeprozedur unterwerfen. [2]Diese muss aus einer Identifikation (Benutzerkennung) und einer Authentifikation (Passwort) bestehen. [3]Die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalter-Privilegien einschließt.

3.3. [1]Die für das Wartungspersonal speziellen Benutzerkennungen werden nur für unmittelbare Wartungsarbeiten freigegeben, ansonsten sind sie gesperrt. [2]Die Freigabe erfolgt durch die kirchliche Stelle.

3.4. [1]Das Wartungspersonal hat nur die Zugriffsrechte, die für die Wartung erforderlich sind. [2]Bei der Wartung und Betreuung von Programmen und Dateien mit sensiblen personenbezogenen Daten sind die Zugriffsrechte nach Abschluss der Arbeiten zu sperren.

3.5. Werden Test- und Serviceprogramme auf der DV-Anlage gespeichert, sind diese unter einer besonderen Kennung abzuspeichern.

3.6. [1]Soweit es möglich ist, sollen personenbezogene Daten aus dem direkten Zugriff des Wartungspersonals entfernt werden. [2]Ist für Wartungszwecke ein Zugriff auf diese Daten erforderlich, ist zu prüfen, ob sensible personenbezogene Daten aus dem direkten Zugriff entfernt werden können. [3]Im Rahmen der Fernwartung ist der Zugriff auf besonders sensible personenbezogene Daten (z. B. Patientendaten aus Beratungsstellen) grundsätzlich zu verhindern.

3.7. [1]Das Einspielen von Änderungen ins Betriebssystem, in systemnahe Software oder in Anwendungsprogramme darf im Rahmen der externen Fernwartung nur nach vorheriger Abstimmung mit der Systembetreuung der kirchlichen Stelle zugelassen werden. [2]Das Gleiche gilt für die Fehlerbehebung. [3]Die Wartung von Programmen und Dateien mit besonders sensiblen personenbezogenen Daten (z. B. Patientendaten der Krankenhäuser) sollte nur vor Ort erfolgen (siehe auch 8.4). [4]Bei der Wartung und Systembetreuung darf es nicht vorkommen, dass die von der kirchlichen Stelle entwickelte Software und die erstellten Dateien durch die Wartung verändert werden können.

3.8. Es ist kritisch zu hinterfragen, inwieweit Wartungs- und Diagnosearbeiten im laufenden Betrieb vorgenommen werden können.

4. Maßnahmen zur Benutzerkontrolle

4.1. Fernwartungspasswörter, die für die Wartung von Programmen und Dateien mit sensiblen personenbezogenen Daten eingesetzt werden, sollen bei der Wartung und Systembetreuung außer Haus nur verschlüsselt übertragen werden.

5. Maßnahmen zur Zugriffskontrolle

5.1. Soweit für Wartungsarbeiten die DV-Anlage oder Softwareprodukte mit den hinterlegten Passwörtern außer Haus gegeben wurden, sind nach Rückgabe der DV-Geräte alle Passwörter zu ändern.

6. Maßnahmen zur Transportkontrolle

6.1. Die Übertragung sensibler personenbezogener Daten auf leitungsgebundenen oder drahtlosen Übertragungswegen ist durch ein kryptografisches Verfahren (Verschlüsselung) zu sichern.

6.2. Beim Transport von Datenträgern mit sensiblen personenbezogenen Daten sind der Transportweg (z. B. verschlossene Behältnisse) und die am Transport beteiligten Personen schriftlich festzulegen.

6.3. Beim Transport von Datenträgern und PC-Geräten sind Nachweise über den Versand zu führen (Begleitzettel, Versandscheine, Empfangsbestätigung).

6.4. [1]Bei Rückgabe von DV-Geräten wird die Vollständigkeit geprüft und dokumentiert. [2]Sofern Programme oder Dateien mit sensiblen personenbezogenen Daten zurückgegeben werden, sind alle Dateien oder DV-Programme auf Integrität zu prüfen.

7. Gemeinsame Maßnahmen zur Zugangs-, Benutzer-, Zugriffs-, Übermittlungs- und Eingabekontrolle

7.1. Alle Fernwartungsaktivitäten sind zu protokollieren (Beginn und Ende der Arbeiten, ausführende Person, Art des Vorgangs und Merkmale der Maßnahme – z. B. Maßnahmen der Systemgenerierung und der Modifikation von Systemparametern, das Einrichten von Wartungspersonen als Benutzerinnen und Benutzer, die Verwaltung von Befugnistabellen, das Einspielen und die Änderung von Anwendungssoftware, die Änderung an der Dateiorganisation, die Durchführung von Backups, Restore- und sonstigen Datensicherungsmaßnahmen, der Aufruf von Administrations-Tools, Dateiübermittlungen).

7.2. [1]Die Protokolle sind sicher aufzubewahren. [2]Die Aufbewahrungsdauer sollte eine Frist von einem Jahr nicht überschreiten. [3]Aufgrund der engen Zweckbindung dürfen Protokolldaten nur für die dazu befugten Personen (Verantwortliche, systemadministrierende Personen, kirchliche Datenschutzbeauftragte) genutzt werden.

8 . Maßnahmen zur Organisationskontrolle

8.1. Die mit der Wartung oder Systembetreuung beauftragten Firmen oder Personen sind sorgfältig auszuwählen.

8.2. [1]Im Wartungsvertrag sind Art und Umfang der Wartung für Hard- und Software sowie ggf. der Ort, von wo aus die Fernwartung durchgeführt wird, schriftlich zu vereinbaren. [2]Umfasst der Wartungsvertrag auch die Wartung und Betreuung von DV-Programmen oder Dateien mit sensiblen personenbezogenen Daten, sind die Rechte und Pflichten zwischen Wartungspersonal und den Mitarbeiterinnen und Mitarbeitern der kirchlichen Stelle festzulegen.

8.3. Das Wartungspersonal ist schriftlich auf das Datengeheimnis nach § 6 DSG-EKD[1] zu verpflichten.

8.4. [1]Bei der Wartung von Programmen und Dateien mit besonders sensiblen personenbezogenen Daten (z. B. Patientendaten aus Beratungsstellen) hat die kirchliche Stelle darauf zu achten, dass nur autorisiertes Wartungspersonal Zugang zum DV-System hat. [2]Von der Durchführung der Fernwartung sollte möglichst abgesehen werden (siehe auch 3.7).

8.5. [1]Bei Durchführung der Wartungsarbeiten außer Haus ist zu prüfen, ob und inwieweit die personenbezogenen Daten zur Fehlersuche und -behebung benötigt werden. [2]Ist dies nicht der Fall, sind sie vor Beginn der Wartung zu löschen. [3]Ansonsten ist zu prüfen, ob die Wartung auch mit Testdaten oder mit anonymisierten oder pseudonymisierten Originaldaten durchgeführt werden kann. [4]Ggf. ist vor einer Übergabe oder Übertragung von Originaldaten die Erlaubnis der Fachabteilung einzuholen.

8.6. [1]Eine Weitergabe von Daten, die dem Wartungspersonal übergeben oder bei der Fernwartung übertragen wurden, an Dritte ist vertraglich zu untersagen. [2]Diese Daten sind ausschließlich für Zwecke der Wartung zu verwenden und nach Abschluss der Wartungsarbeiten oder der Fehlersuche unverzüglich zu löschen. [3]Für evtl. weitergegebene Listen mit personenbezogenen Daten ist eine Rückgabe oder die sachgerechte Vernichtung nach Abschluss der Wartungsarbeiten zu vereinbaren.

8.7. Es ist schriftlich zu vereinbaren, dass Schadensansprüche von betroffenen Personen (z. B. nach § 8 DSG-EKD[2]) von den wartenden Personen oder Firmen zu tragen sind, wenn personenbezogene oder sonstige schützenswerte Daten vom Wartungspersonal unzulässigerweise offenbart wurden.

---

1 Nr. **850**
2 Nr. **850**.

8.8. [1]Bei der Wartung und Systembetreuung vor Ort sind Regelungen über die Beaufsichtigung des Wartungspersonals zu treffen. [2]Beim Umgang mit Programmen und Dateien mit sensiblen personenbezogenen Daten sollte möglichst eine fachkundige Kraft anwesend sein. [3]In einem Tätigkeitsprotokoll sind die durchgeführten Aktivitäten aufzuzeichnen.

8.9. Nach Abschluss der Wartungsarbeiten ist routinemäßig ein Viren-Check durchzuführen.

8.10. Die systemadministrierenden Personen der kirchlichen Stelle sollten auch bezüglich der Gefahren der Fernwartung geschult werden.

8.11. Die kirchliche Stelle überprüft regelmäßig die Einhaltung der vereinbarten Sicherheitsmaßnahmen.

8.12. Die kirchliche Stelle sollte das Wartungs- bzw. Fernwartungskonzept schriftlich dokumentieren.

Anlage 2

CHECKLISTE *

Datenschutz bei externer Wartung und Systembetreuung

Stand: 01.12.2000

A. V e r t r a g s g r u n d l a g e n

Informationen und Unterlagen
Welche externen Personen und Firmen führen Wartungs- und Systembetreuungsarbeiten durch: 1. ..... 2. ..... 3. ..... 4. ..... 5. .....
Wartungsvertrag vom *(ggf. als Anlage beifügen)*: Zu 1.: ..... Zu 2.: ..... Zu 3.: ..... Zu 4.: ..... Zu 5.: .....

Informationen und Unterlagen
Wartungsbereich *(bitte betroffene Hard- und Software angeben)*:
Zu 1.: .....
Zu 2.: .....
Zu 3.: .....
Zu 4.: .....
Zu 5.: .....
Um welche Art von Wartung handelt es sich:
Zu 1.: □ Arbeiten vor Ort □ Wartungs- u. Systembetreuung außer Ort □ Fernwartung
Zu 2.: □ Arbeiten vor Ort □ Wartungs- u. Systembetreuung außer Ort □ Fernwartung
Zu 3.: □ Arbeiten vor Ort □ Wartungs- u. Systembetreuung außer Ort □ Fernwartung
Zu 4.: □ Arbeiten vor Ort □ Wartungs- u. Systembetreuung außer Ort □ Fernwartung
Zu 5.: □ Arbeiten vor Ort □ Wartungs- u. Systembetreuung außer Ort □ Fernwartung
In welchem Umfang wird die Wartung durchgeführt:
Zu 1.: □ Gelegentlich bei Bedarf □ Regelmäßig □ Wartungspersonal ist ständig vor Ort
Zu 2.: □ Gelegentlich bei Bedarf □ Regelmäßig □ Wartungspersonal ist ständig vor Ort
Zu 3.: □ Gelegentlich bei Bedarf □ Regelmäßig □ Wartungspersonal ist ständig vor Ort
Zu 4.: □ Gelegentlich bei Bedarf □ Regelmäßig □ Wartungspersonal ist ständig vor Ort
Zu 5.: □ Gelegentlich bei Bedarf □ Regelmäßig □ Wartungspersonal ist ständig vor Ort

Bemerkungen: .....

.....

.....

.....

Klassifizierung der Schutzstufe

[1]*Personenbezogene Daten* werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Missbrauch dieser Daten in 5 Schutzstufen untergliedert. [2]Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. [3]Die Betrachtung ist vielmehr auf die gesamte Datei bzw. auf das DV-Programm auszudehnen. [4]Enthalten Dateien umfassende Angaben zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre.

Es ist aber auch denkbar, dass der Schutz empfindlicher Daten ohne Personenbezug (z. B. Finanzentwicklung, Struktur- und Planungskonzepte) die Einstufung bestimmt.

Es werden folgende Schutzstufen unterschieden:

Stufe A:	Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z. B. Adressbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.
Stufe B:	Personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z. B. beschränkt zugängliche kirchliche Dateien, Verteiler für Unterlagen.
Stufe C:	Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann („Ansehen“), z. B. Einkommen, Sozialleistungen.
Stufe D:	Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann („Existenz“), z. B. Unterbringung in Anstalten, Straffälligkeit, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse, Patientendaten aus kirchlichen Beratungsstellen oder Krankenhäusern.
Stufe E:	Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann.

Stufe	Dateien/DV-Programme *(ggf. Einstufung begründen)*
Stufe A	
Stufe B	
Stufe C	
Stufe D	
Stufe E	

B. Technische und organisatorische Sicherheitsmaßnahmen

[1]Die einzelnen Anforderungen sind nach dem Schutzstufenkonzept gestaffelt aufgeführt. [2]Die Grundschutzforderungen unter der Schutzstufe A-B sind immer anzuwenden. [3]Die unter den Schutzstufen C, D oder E aufgeführten Anforderungen kommen auf Grund der höheren Datenschutzsicherungsanforderung jeweils ergänzend hinzu.

1	**Allgemeine Anforderungen**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
Daten der Schutzstufe A-B:					
1.1	Die mit der Wartung oder Systembetreuung beauftragten Firmen oder Personen sind sorgfältig ausgewählt worden. Art und Umfang der Wartung für Hard- und Software sind vertraglich vereinbart.				
1.2	Das Wartungspersonal ist schriftlich auf das Datengeheimnis verpflichtet (§§ 6, 11 DSG-EKD).				
1.3	Die Weitergabe der Daten, die dem Wartungspersonal übergeben wurden, an Dritte ist untersagt.				
1.4	Es ist schriftlich vereinbart, dass Schadensansprüche von betroffenen Personen (z. B. nach § 8 DSG-EKD) von den beauftragten Personen oder Firmen zu tragen sind, wenn personenbezogene oder sonstige schützenswerte Daten vom Wartungspersonal unzulässigerweise offenbart wurden.				

1	**Allgemeine Anforderungen**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
1.5	Die Wartungsarbeiten beginnen erst auf Anforderung.				
1.6	Das Wartungspersonal arbeitet mit Datenträgern der kirchlichen Stelle; mitgebrachte Datenträger verbleiben für einen bestimmten Zeitraum bei der kirchlichen Stelle für Kontrollzwecke.				
1.7	Soweit möglich sind personenbezogene Daten aus dem direkten Zugriff des Wartungspersonals entfernt worden.				
1.8	Alle Wartungs- und Übertragungsaktivitäten sollten i. d. R. am Bildschirm zum Mitlesen sichtbar sein oder in einem Tätigkeitsprotokoll aufgezeichnet werden.				
1.9	Die Wartungsarbeiten können jederzeit durch die kirchliche Stelle abgebrochen werden.				
1.10	Die weitergegebenen personenbezogenen Daten, Listen etc. werden nach Abschluss der Wartungsarbeiten unverzüglich gelöscht oder zurückgegeben.				
1.11	Nach Abschluss der Wartungsarbeiten wird ein Viren-Check durchgeführt.				

1	Allgemeine Anforderungen	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungen zu den Wartungsverträgen
1.12	[1]Die systemadministrierenden Personen besitzen zumindest Grundkenntnisse, um die Tätigkeiten des Wartungspersonals nachvollziehen zu können. [2]Sie sind regelmäßig bezüglich der Gefahren der Fernwartung zu schulen.				
1.13	Die kirchliche Stelle überprüft regelmäßig die Einhaltung der vereinbarten Sicherheitsmaßnahmen.				
Daten der Schutzstufe C:					
1.14	Ein Sicherheitskonzept liegt bei der kirchlichen Stelle vor.				
1.15	Das Wartungspersonal hat nur die Zugriffsrechte, die für die Wartung erforderlich sind.				
1.16	Bei entsprechender Notwendigkeit ist ein Fristenplan für regelmäßige Wartungsarbeiten aufzustellen.				
1.17	[1]Die speziellen Benutzerkennungen werden nur für unmittelbare Wartungsarbeiten freigegeben, ansonsten sind sie gesperrt. [2]Die Freigabe erfolgt durch die kirchliche Stelle.				

1	**Allgemeine Anforderungen**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
1.18	Werden Test- und Serviceprogramme auf der DV-Anlage gespeichert, sind diese unter einer besonderen Kennung abzuspeichern.				
1.19	Art und Umfang der einzelnen Wartungsarbeiten werden schriftlich in einem Tätigkeitsprotokoll festgehalten (Namen der Wartungspersonen, Zeitpunkt, Aktionen, Ergebnisse).				
1.20	Die dem Wartungspersonal eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind nach Abschluss der Arbeiten widerrufen bzw. gesperrt oder gelöscht worden.				
Daten der Schutzstufe D:					
1.21	Der Kreis der Zugangs- und Zugriffsberechtigten ist schriftlich festgelegt.				
Daten der Schutzstufe E:					
1.22	Die Autorisierung des Wartungspersonals wird vom Auftraggeber überprüft.				

2	**Wartung und Systembetreuung vor Ort** **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
Daten der Schutzstufe A-B:					
2.1	Die Wartungspersonen weisen sich vor Beginn der Arbeiten aus, soweit sie nicht persönlich bekannt sind.				
2.2	Die dem Wartungspersonal eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum beschränkt.				
2.3	[1]Die Software-Änderungen (einschl. Fehlerbehebung) werden nur nach vorheriger Abstimmung mit der Systembetreuung der kirchlichen Stelle eingespielt. [2]Wesentlich geänderte Programmversionen sollten vorher freigegeben worden sein. [3]Die von der kirchlichen Stelle entwickelte Software und die erstellten Dateien werden durch die Wartung nicht verändert.				
Daten der Schutzstufe C:					
2.4	Regelungen über die Beaufsichtigung des Wartungspersonals liegen vor.				
Daten der Schutzstufe D:					
2.5	Das Wartungspersonal wird ständig überwacht.				

2	**Wartung und Systembetreuung vor Ort** **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
2.6	Die Wartungsperson nimmt keine am DV-System erzeugten Datenträger ungelöscht mit.				
2.7	Die Zutritts- und Zugangsrechte für das Wartungspersonal sind nach Abschluss der Arbeiten zu sperren.				

3	**Externe Wartung und Systembetreuung außer Haus** **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
Daten der Schutzstufe A-B:					
3.1	[1]Werden personenbezogene Daten zu Wartungszwecken oder zur Fehleranalyse benötigt, ist zu prüfen, ob sie anonymisiert, pseudonymisiert[1] bzw. ganz oder teilweise gelöscht werden können. [2]Ausnahmen sind schriftlich begründet; die Fachabteilung hat zugestimmt.				

1 Siehe Fußnote bei Anlage 1 und 2.

3	**Externe Wartung und Systembetreuung außer Haus** **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
3.2	Es werden Nachweise über den Versand geführt (Begleitzettel, Versandscheine, Empfangsbestätigung).				
3.3	Bei Rückgabe der Geräte wird die Vollständigkeit geprüft und dokumentiert.				
3.4	Alle Passwörter der DV-Anlage oder der Softwareprodukte werden nach Rückgabe der Geräte geändert.				
Daten der Schutzstufe D:					
3.5	Der Transportweg und die am Transport beteiligten Personen sind schriftlich festgelegt.				
3.6	Alle Dateien oder Softwareprodukte sind nach Rückgabe auf Integrität geprüft.				

	Fernwartung **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
Daten der Schutzstufe A-B:					
4.1	[1]Werden personenbezogene Daten zu Wartungszwecken oder zur Fehleranalyse benötigt, ist zu prüfen, ob sie anonymisiert, pseudonymisiert[1] bzw. ganz oder teilweise gelöscht werden können. [2]Ausnahmen sind schriftlich begründet; die Fachabteilung hat zugestimmt.				
4.2	Es sind Passwörter für die Fernwartung sowie Art und Umfang der Berechtigungen für die wartenden Personen festzulegen.				
4.3	Der Verbindungsaufbau erfolgt seitens der kirchlichen Stelle zu der vorher festgelegten Telefonnummer des Wartungsunternehmens.				
4.4	Der Dialog mit der Fernwartungszentrale wird unterbrochen, wenn die Verbindung zur Fernwartungszentrale gestört ist („Zwangslogout“).				
4.5	[1]Alle Fernwartungsaktivitäten werden protokolliert. [2]Die Protokolle werden sicher für einen vorher bestimmten Zeitraum aufbewahrt.				

1 Siehe Fußnote bei Anlage 1 zu 2.

	Fernwartung **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
4.6	Dateien oder Programme werden von der Fernwartungsstelle nur nach vorheriger Absprache angelegt.				
Daten der Schutzstufe C:					
4.7	Fernwartungspasswörter werden nur verschlüsselt übertragen.				

	Fernwartung **– zusätzliche Datenschutzmaßnahmen –**	**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungen zu den Wartungsverträgen**
Daten der Schutzstufe C:					
4.8	[1]Die Software-Änderungen (einschl. Fehlerbehebung) werden nur nach vorheriger Abstimmung mit der Systembetreuung der kirchlichen Stelle eingespielt. [2]Wesentlich geänderte Programmversionen sollten vorher freigegeben worden sein. [3]Die von der kirchlichen Stelle entwickelte Software und die erstellten Dateien werden durch die Wartung nicht verändert.				
4.9	Die Übertragung personenbezogener Daten auf leitungsgebundenen oder drahtlosen Übertragungswegen ist durch ein kryptografisches Verfahren gesichert.				
Daten der Schutzstufe E:					
4.10	Bei Verarbeitung von personenbezogenen Daten der Schutzstufe E wird keine Fernwartung durchgeführt.				

Anlage 3

Empfehlungen der Evangelischen Kirche von Westfalen
zur datenschutzrechtlichen Gestaltung
von Fernwartungsverträgen

– Stand 01.12.2000 –

Vorbemerkung:

[1]Auf Grundlage des Schreibens der Evangelischen Kirche von Westfalen vom 22.08.2000, Az.: A 14 – 03/01.09, das konkrete Hinweise und Handlungsempfehlungen zum Datenschutz bei Inanspruchnahme externer Wartung und Systembetreuung enthält, wurden die Empfehlungen zur datenschutzrechtlichen Gestaltung von Fernwartungsverträgen entwickelt. [2]Die folgenden Klauseln sind als Formulierungshilfen gedacht und beziehen sich vorrangig auf die Bereiche Datenschutz und Datensicherheit. [3]Unter Berücksichtigung der Vorgaben des Schutzstufenkonzeptes der Checkliste „Datenschutz bei externer Wartung und Systembetreuung“ (siehe Anlage 2 des o. a. Schreibens) sind einzelne Pflichten des Auftragnehmers der Sensibilität der personenbezogenen Daten anzupassen. [4]Es ist zu prüfen, ob die Empfehlungen zur datenschutzrechtlichen Gestaltung von Fernwartungsverträgen in die von den Wartungs- und Systembetreuungsfirmen vorgelegten Verträge eingearbeitet werden können. [5]Ansonsten wäre eine Zusatzvereinbarung erforderlich, wobei die Punkte des Wartungsvertrages konkret zu bezeichnen sind, die durch die Zusatzvereinbarung berührt und gegebenenfalls gegenstandslos werden.

1. Art und Umfang der Wartung

Es sind festzulegen:

- das zu wartende System (Hard- und Software) mit Standort sowie die betroffenen DV-Programme und Datenbestände;
- Art der Wartung (nur Fernwartung, nur vor Ort, beides) sowie Beschreibung der Fälle, in denen Fernwartung betrieben werden darf;
- Beschreibung der Wartungsarbeiten, der Funktionalität und der technischen Gestaltung (z. B. welche Softwareupdates vorgenommen werden sollen – ein Update, das ausschließlich zur Fehlerbehebung dient, ist verhältnismäßig unproblematisch; eine neue Programmversion mit wesentlichen Verfahrensänderungen bedarf der vorherigen Freigabe der kirchlichen Stelle);
- Wartungsbereitschaft und Reaktionszeit (z. B. permanent, Wochenende ausgeschlossen, Montag bis Freitag von 7.00 Uhr bis 18.00 Uhr, Reaktionszeit innerhalb einer Stunde oder innerhalb von sechs Stunden).

2. Laufzeit, Kündigung, Vertragsende

Es sind festzulegen:

- Geltungsdauer des Vertrages
- Automatische Verlängerung
- Fälle der ordentlichen und außerordentlichen Kündigung
- [1]Mit Beendigung des Wartungs- und Systembetreuungsvertrages hat der Auftragnehmer alle Unterlagen, die personenbezogene Daten aus Dateien oder Programmen der kirchlichen Stelle enthalten, der kirchlichen Stelle zurückzugeben. [2]Die Datenträger des Auftragnehmers sind danach physisch zu löschen. [3]Listen mit personenbezogenen Daten sind unverzüglich zu vernichten oder zurückzugeben.

3. Vergütung

…

4. Pflichten des Auftragnehmers

Der Auftragnehmer führt Wartungs- und Systembetreuungsarbeiten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der kirchlichen Stelle durch.

Weisungsberechtigte Personen des Auftraggebers (kirchliche Stelle) sind:

1. …
2. …
3. …

Weisungsempfänger beim Auftragnehmer sind:

1. …
2. …
3. …

Bei einem Wechsel oder einer längerfristigen Verhinderung der weisungsberechtigten bzw. weisungsempfangenden Personen sind dem Vertragspartner unverzüglich schriftlich die vertretenden oder nachfolgenden Personen mitzuteilen.

[1]Die Einschaltung von Sub-Auftragnehmern ist ausgeschlossen. [2]Die Hinzuziehung von anderen sachverständigen Personen zur Fehlerbehebung bedarf der vorherigen Zustimmung der kirchlichen Stelle.

4.1 Geltung der kirchlichen Datenschutzbestimmungen, Datengeheimnis

[1]Der Auftragnehmer beachtet die kirchlichen Datenschutzbestimmungen. [2]Der Auftraggeber (kirchliche Stelle) stellt dem Auftragnehmer die derzeit geltenden kirchlichen Da-

tenschutzbestimmungen zur Verfügung und wird den Auftragnehmer über Änderungen des Datenschutzrechtes schriftlich informieren.

[1]Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Wartungs- und Systembetreuungsarbeiten beschäftigten Personen mit den für sie maßgebenden Bestimmungen des kirchlichen Datenschutzes vertraut macht. [2]Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

[1]Der Auftragnehmer verpflichtet sich, das Datengeheimnis nach § 6 DSG-EKD[1] zu beachten, wonach es den bei der Datenverarbeitung beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. [2]Das Wartungspersonal ist schriftlich auf das Datengeheimnis zu verpflichten.

Auskünfte an Dritte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch die kirchliche Stelle erteilen.

4.2 Kontrollrecht des kirchlichen Datenschutzbeauftragten

Der Auftragnehmer verpflichtet sich, dem Datenschutzbeauftragten der Evangelischen Kirche von Westfalen Zugang zu den Arbeitsräumen zu gewähren und Auskunft zu erteilen, soweit personenbezogene Daten der kirchlichen Stelle dort vorgehalten werden.

4.3 Datenschutzregelungen beim Auftragnehmer

[1]Der Auftragnehmer dokumentiert die von ihm getroffenen aktuellen technischen und organisatorischen Datenschutzmaßnahmen in der Anlage zum Wartungsvertrag. [2]Die Anlage ist Bestandteil dieses Vertrages (z. B. verschlüsselte Verbindung, Unbefugte haben keinen Zugang zu den Geschäftsräumen und zu den PCs der Wartungsfirma).

4.4 Technisch-organisatorische Regelungen sowie Maßnahmen zum Datenschutz und zur Datensicherheit

[1]Wartungs- und Systembetreuungsarbeiten dürfen vor Ort erst durchgeführt werden, wenn die systemverwaltenden Personen der kirchlichen Stelle ihre Zustimmung erteilt haben. [2]Vom Auftragnehmer mitgebrachte und für die Wartung benutzte Datenträger verbleiben für einen Zeitraum von sechs Monaten bei der kirchlichen Stelle für Kontrollzwecke. [3]Art und Umfang der einzelnen Wartungsarbeiten werden schriftlich in einem Tätigkeitsprotokoll festgehalten (Namen der Wartungspersonen, Zeitpunkt, Aktionen, Ereignisse).

Der Auftragnehmer verpflichtet sich, die von der kirchlichen Stelle entwickelte eigene Software und die erstellten Dateien durch die Wartungs- und Systembetreuungsarbeiten nicht zu verändern.

Soweit sensible personenbezogene Daten auf leitungsgebundenen oder drahtlosen Wegen zum Auftragnehmer hin übertragen werden sollen, sind die Daten durch ein kryptografisches Verfahren (Verschlüsselung) zu sichern.

---

1 Nr. **850**.

[1]Für den Transport von Datenträgern und PC-Geräten zwischen dem Auftragnehmer und dem Auftraggeber, auf denen sensible personenbezogene Daten enthalten sind, sind gesonderte Sicherheitsmaßnahmen zu vereinbaren. [2]Bei der Übergabe von DV-Geräten wird vom Auftragnehmer die Vollständigkeit geprüft und dokumentiert.

[1]Der Verbindungsaufbau für die Fernwartung oder die Fernwartungsfreigabe im Betriebs- oder Anwendungssystem erfolgt durch die systemverwaltenden Personen der kirchlichen Stelle (z. B. Einschaltung des Modems, Aktivierung der Benutzerkennung für die Wartung). [2]Wird die Verbindung eine gewisse Zeit nicht genutzt (Zeitintervall muss einstellbar sein), wird der Verbindungsaufbau bzw. die Fernwartungsfreigabe durch die kirchliche Stelle abgebrochen, sonst unverzüglich nach Ende der Wartungsarbeiten. [3]Eine Fernwartung darf nur stattfinden, während die systemverwaltenden Personen der kirchlichen Stelle anwesend sind, die gegebenenfalls den Netz- oder PC-Zugang sperren können. [4]Durch ihre Anwesenheit soll auch sichergestellt werden, dass sie die ablaufenden Vorgänge und Änderungen kontrollieren können.

Die Durchführung der Fernwartung von einer Privatwohnung aus ist nicht zulässig.

Vor Beginn der Fernwartung absolviert das Wartungspersonal des Auftragnehmers eine Anmeldeprozedur mit Authentisierung (mindestens Benutzerkennung und Passwort).

[1]Der Auftragnehmer stellt die technischen Möglichkeiten zur Protokollierung aller Aktivitäten des Wartungsvorgangs zur Verfügung. [2]Der Wartungsvorgang wird von dem Auftragnehmer so gestaltet, dass er auf der Konsole des PCs der Systemverwaltung der kirchlichen Stelle mitverfolgt werden kann. [3]Der Auftragnehmer protokolliert den Anlass und die im Einzelnen durchgeführten Maßnahmen der Wartung und stellt den systemverwaltenden Personen der kirchlichen Stelle das Protokoll unverzüglich zur Verfügung. [4]Die Protokolle werden beim Auftragnehmer für mindestens ein Jahr aufbewahrt.

[1]Der Auftragnehmer verpflichtet sich, bei normalen Wartungs- und Systembetreuungsarbeiten auf personenbezogene Daten nicht zuzugreifen. [2]Die Lösung von Problemfällen hat vorrangig in Testumgebungen stattzufinden, möglichst mit anonymisierten oder pseudonymisierten personenbezogenen Daten. [3]Sollte ein Zugriff auf Programme der kirchlichen Stelle unabdingbar sein, darf dies nur mit Einwilligung der systembetreuenden Personen der kirchlichen Stelle erfolgen. [4]Die Übertragung personenbezogener Daten zum Auftragnehmer per Dateitransfer oder Download ist nicht gestattet und bedarf in begründeten Ausnahmefällen der Zustimmung der systemverwaltenden Personen der kirchlichen Stelle. [5]Kopien oder Duplikate von Dateien oder Programmen mit personenbezogenen Daten dürfen nur mit der Zustimmung der kirchlichen Stelle erstellt werden.

[1]Die bei der Fernwartung ausnahmsweise übertragenen personenbezogenen Daten dürfen an keinen Dritten weitergegeben werden. [2]Diese Daten sind ausschließlich für Zwecke der Wartung zu verwenden und nach Abschluss der Wartungsarbeiten oder der Fehlersuche unverzüglich zu löschen. [3]Listen mit personenbezogenen Daten sind ebenfalls nach Ab-

schluss der Wartungsarbeiten entweder sachgerecht zu vernichten oder an die kirchliche Stelle zurückzugeben.

Der Auftraggeber informiert die kirchliche Stelle unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei den vereinbarten Datenschutz- und Datensicherungsmaßnahmen feststellt.

[1]Der Auftragnehmer unterrichtet die kirchliche Stelle unverzüglich, wenn eine von der kirchlichen Stelle erteilte Weisung nach seiner Meinung zu einem Verstoß gegen kirchliche oder staatliche Vorschriften führen kann. [2]Die Weisung braucht nicht befolgt zu werden, so lange sie nicht durch die kirchliche Stelle geändert oder ausdrücklich bestätigt wird.

Soweit die beim Auftragnehmer oder Auftraggeber getroffenen Sicherheitsmaßnahmen den Anforderungen des kirchlichen Datenschutzes nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

[1]Die technischen und organisatorischen Datenschutz- und Datensicherungsmaßnahmen können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. [2]Wesentliche Änderungen und solche, die den Vertrag direkt berühren, sind schriftlich zu vereinbaren.

4.5 Haftung

Der Auftragnehmer haftet gegenüber der kirchlichen Stelle für Schäden, die er oder seine Mitarbeitenden schuldhaft verursachen.

[1]Für den Ersatz von Schäden, die eine betroffene Person gegenüber der kirchlichen Stelle – insbesondere nach § 8 DSG-EKD[1] – geltend macht, ist die kirchliche Stelle gegenüber dem Betroffenen verantwortlich. [2]Soweit die kirchliche Stelle aufgrund von Schäden, die der Auftragnehmer nach Satz 1 zu vertreten hat, zum Schadensersatz gegenüber den betroffenen Personen verpflichtet ist, bleibt der kirchlichen Stelle der Rückgriff auf den Auftragnehmer vorbehalten.

4.6 Vertragsstrafe

Bei Verstoß gegen wesentliche Bestimmungen dieses Vertrages (4.1, 4.2, 4.3, 4.4) kann der Auftraggeber (kirchliche Stelle) vom Auftragnehmer eine Vertragsstrafe in Höhe von ..... Euro geltend machen.

1 Nr. **850**.