Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland

Arbeitshilfe mit Erläuterungen zur Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11Datenschutzgesetz-EKD (DSG-EKD)

Metadaten:

Version:	1.1
Ausgabedatum:	07. September 2016
Status:	☐ in Bearbeitung
	☐ in Abstimmung
	☑ Freigegeben
Ansprechpartner juristisch:	Der Beauftragte für den Datenschutz der EKD 0511 762128-0 info@datenschutz.ekd.de
Ansprechpartner technisch:	keiner

Inhaltsübersicht

A. Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11 Datenschutzgesetz-EKD (DSG-EKD) (Auftragsdatenverarbeitung – ADV)

zwischen

Name der kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

(nachfolgend **„Auftraggeber“** genannt)

und

Dienstleister

Straße Hausnummer

Postleitzahl Ort

(nachfolgend **„Auftragnehmer“** genannt)

– nachstehend gemeinsam auch Parteien genannt –

Präambel

Die vorliegende Vereinbarung – im Folgenden „ADV“ genannt – konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien aus § 11 DSG-EKD, die sich aus der Auftragsdatenverarbeitung basierend auf dem Dienstleistungsvertrag vom [Datum] (nachstehend „Hauptvertrag“ genannt) ergeben.

Ziel ist die datenschutzgerechte Durchführung der [Beschreibung der Dienstleistungsaufgabe]. Der Inhalt des Vertrages bezieht sich auf den Umgang mit personenbezogenen Daten (im Folgenden „Daten“ genannt), die der Auftraggeber an den Auftragnehmer übergibt bzw. die im Auftrag des Auftraggebers erhoben, verarbeitet oder genutzt werden. Der Vertrag gilt für alle Tätigkeiten und Anwendungen, bei denen Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit diesen personenbezogenen Daten in Berührung kommen können. Für rechtliche hier nicht näher definierte Begriffe oder Ausdrücke gelten die maßgeblichen gesetzlichen Definitionen des DSG-EKD.

§ 1
Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung:

(2) Diese Vereinbarung gilt ab dem 03.03.2015 und endet nach der Beendigung des Hauptvertrages mit der Übergabe oder der Vernichtung aller personenbezogenen Daten des Auftraggebers gemäß § 10 dieser Vereinbarung, ohne dass es einer gesonderten Kündigung dieser Vereinbarung dazu bedarf.

[(3) Die Vereinbarung gilt entsprechend für (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Insoweit gilt § 11 ADV.]

§ 2
Konkretisierung des Auftragsinhalts

(1) Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle gemäß § 11 Absatz 1 Satz 1 DSG-EKD.

(2) Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten, die Art der Daten und der Kreis der Betroffenen wird wie folgt festgelegt:

1. Art der Daten

Gegenstand der Erhebung, Verarbeitung oder Nutzung von Daten [dazu gehören auch neu entstehende Daten] durch den Auftragnehmer sind folgende Datenarten bzw. -kategorien:

Daten aus der [Aufzählung, Beschreibung der Datenkategorien, z. B. Personenstammdaten, Kommunikationsdaten wie etwa Telefonnummern, E-Mail-Adressen, Vertragsstammdaten wie etwa Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten, Beispiel Buchhaltung: Rechnungsdaten, Lieferantendaten, Debitoren und Kreditoren, Adressdaten, Bankverbindungen, Gläubiger-ID nach SEPA, Ansprechpartner bei Lieferanten, Telefonnummern, Steuernummern]

2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber sind in den folgenden Dokumenten näher beschrieben:

[Aufzählung der Dokumente, z. B. Leistungsvereinbarung]

bzw. werden wie folgt näher beschrieben:

[Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Datenverarbeitung durch den Auftragnehmer]

3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst [Aufzählung/Beschreibung der betroffenen Personenkategorien, z. B. Gemeindeglieder, Patienten, Mitarbeitende, Abonnenten, Lieferanten, Pächter, Mieter, Ansprechpersonen]

§ 3
Technische und organisatorische Maßnahmen

(1) Die Erhebung, Verarbeitung oder Nutzung von Daten durch den Auftragnehmer findet nur auf Datenverarbeitungsanlagen statt, für die technische und organisatorische Maßnahmen zum Schutz der Daten getroffen wurden. In diesem Zusammenhang verpflichtet sich der Auftragnehmer, auf seine Kosten alle Maßnahmen gemäß der Anlage zu § 9 Abs. 1 DSG-EKD zu treffen, die für die Erfüllung des in § 1 beschriebenen Auftrages erforderlich sind. Die in diesem Sinne derzeit erforderlichen und vom Auftragnehmer getroffenen Maßnahmen sind in Anlage 1 zur ADV festgehalten und werden als verbindlich festgelegt.

(2) Insgesamt handelt es sich bei den Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, des Trennungsgebots und der Organisationskontrolle sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs und Bereitstellung von Daten, Art und Umstände der Verarbeitung, die Datenhaltung sowie Art und Umstände beim Output und Datenversand.

Im Rahmen der Zugangs-, Zugriffs- und Weitergabekontrolle hat der Auftragnehmer Verschlüsselungsverfahren einzusetzen, die dem aktuellen Stand der Technik entsprechen.

Der Auftragnehmer stellt dem Auftraggeber das aktuelle IT-Sicherheitskonzept zur Verfügung.

(3) Die oben beschriebenen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Soweit diese aus Sicht des Auftragnehmers durch technischen Fortschritt unwirtschaftlich geworden sind oder keinen zeitgemäßen Schutz mehr bieten, benachrichtigt der Auftragnehmer den Auftraggeber.

Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Andererseits ist der Auftraggeber in einem solchen Fall berechtigt, Anpassungen der Sicherheitsmaßnahmen durch den Auftragnehmer zu veranlassen. Bei der Durchführung der erforderlichen Anpassungsmaßnahmen ist zu gewährleisten, dass das Sicherheitsniveau der in

Anlage 1 festgelegten Maßnahmen nicht unterschritten, sondern möglichst erhöht wird. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer wird dem Auftraggeber etwaige aktualisierte Fassungen auch ohne gesonderte Aufforderung des Auftraggebers zukommen lassen, die sodann als „neue Anlage 1“ die frühere Anlage 1 ersetzt. Der Auftragnehmer hat auf Anforderung dem Auftraggeber die Angaben nach § 21a DSG-EKD / § 4e BDSG zur Verfügung zu stellen.

(4) Verarbeitet der Auftragnehmer auch andere Daten als solche des Auftraggebers, garantiert der Auftragnehmer, dass diese Daten durch technische und organisatorische Maßnahmen von den Daten des Auftraggebers getrennt sind und bleiben.

§ 4
Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren.

(2) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Auskünfte an Dritte und an Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung seitens des Auftraggebers erteilen.

(3) Ist der Auftraggeber gegenüber einem Betroffenen verpflichtet, diesem Auskünfte zur Auftragsdatenverarbeitung zu erteilen, wird der Auftragnehmer auf eigene Kosten den Auftraggeber bei der Ermittlung der zu diesem Zweck benötigten Informationen unterstützen.

§ 5
Kontrollen und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer stellt in seinem Verantwortungsbereich die Einhaltung der Vorschriften des DSG-EKD und ergänzender Bestimmungen nach § 27 DSG-EKD sowie anderer anwendbarer Vorschriften über den Datenschutz sicher.

Der Auftragnehmer verpflichtet sich, das Datengeheimnis nach § 6 DSG-EKD zu wahren. Der Auftragnehmer setzt für die Datenverarbeitung nur solche Beschäftigten oder sonstigen Personen ein, die gemäß § 6 DSG-EKD unter Hinweis auf die möglichen Folgen auf das Datengeheimnis schriftlich verpflichtet und mit den kirchlichen Datenschutzvorschriften vertraut gemacht worden sind.

Auf Verlangen des Auftraggebers wird der Auftragnehmer die Verpflichtung der Beschäftigten und sonstigen Personen gemäß § 6 DSG-EKD dem Auftraggeber nachweisen.

Der Auftragnehmer überwacht fortlaufend die Einhaltung datenschutzrechtlicher Vorschriften durch die eingesetzten Beschäftigten und sonstigen Personen.

(2) Der Auftragnehmer verwendet die Daten für keine anderen als die in dieser ADV festgelegten Zwecke. Der Auftragnehmer verpflichtet sich, dass die Inhalte, die ihm anlässlich der Auftragsdatenverarbeitung zur Kenntnis gelangt sind, sowie die Arbeitsergebnisse keinem Unbefugten zur Kenntnis gelangen. Diese Verpflichtung besteht auch nach Beendigung des Vertrags fort. Kopien und Duplikate werden nur mit Zustimmung des Auftraggebers erstellt. Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung

erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten durch den Auftragnehmer erforderlich sind, dürfen erstellt werden.

(3) Der Auftragnehmer ist verpflichtet, Kontrollen durch regelmäßige Prüfungen im Hinblick auf die Vertragsausführung bzw. Vertragserfüllung durchzuführen. Dazu gehören auch technische und organisatorische Maßnahmen nach § 3 dieses Vertrages. Dem Auftraggeber sind die Prüfprotokolle auf Verlangen unverzüglich vorzulegen.

(4) Der Auftragnehmer unterstellt sich der Kontrolle der oder des Beauftragten für den Datenschutz der EKD. Die oder der Beauftragte für den Datenschutz der EKD nimmt insbesondere die Aufgaben und Rechte nach § 19 DSG-EKD und § 20 DSG-EKD unmittelbar gegenüber dem Auftragnehmer wahr.

(5) Ist der Auftraggeber verpflichtet, Auskünfte über die Verarbeitung von Daten zu geben, so wird der Auftragnehmer ihn darin unterstützen.

(6) Die Datenverarbeitung durch den Auftragnehmer findet im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung der Datenverarbeitung in einen anderen Mitgliedsstaat der Europäischen Union bedarf der vorherigen schriftlichen Zustimmung durch den Auftraggeber. Dem Auftraggeber steht für den Fall der Verlagerung der Datenverarbeitung in ein anderes Land ein außerordentliches Kündigungsrecht zu.

Der Auftragnehmer hat die konkreten Orte der Leistungserbringung stets aktuell zu dokumentieren und auf Verlangen des Auftraggebers nachzuweisen.

(7) Der Auftraggeber kann jederzeit während des Bestehens des Vertragsverhältnisses schriftlich die Daten herausverlangen. Soweit die Daten auf einem Speichermedium herausgegeben werden, ist der Schutz der Daten durch technische und organisatorische Maßnahmen sicherzustellen.

(8) Die Verarbeitung von Daten in Privatwohnungen ist grundsätzlich nicht zulässig. Ausnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers. Für den jeweiligen Einzelfall sind die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten festzulegen. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber oder die Beauftragte für den Datenschutz der EKD oder den Beauftragten für den Datenschutz der EKD vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(9) Der Auftragnehmer bestätigt, dass er einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt hat und verpflichtet sich, die Bestellung eines betrieblichen Datenschutzbeauftragten während der Dauer des Vertrages aufrechtzuhalten, auch wenn die gesetzlichen Voraussetzungen für eine Bestellpflicht entfallen sollten. Die Kontaktdaten des betrieblichen Datenschutzbeauftragten ergeben sich aus der Anlage 2. Einen Wechsel in der Person des betrieblichen Datenschutzbeauftragten hat der Auftragnehmer dem Auftraggeber unverzüglich schriftlich mitzuteilen.

§ 6
Unterauftragsverhältnisse

(1) Der Auftragnehmer erbringt die nachfolgend aufgeführten Leistungen ausschließlich durch folgende Unterauftragnehmer.

[Art der Leistung, Name und Kontaktdaten]

(2) Die Verträge des Auftragnehmers mit seinen Unterauftragnehmern sind derart gestaltet, dass sie den Anforderungen der jeweils anwendbaren gesetzlichen Bestimmungen über den Datenschutz genügen und dass die Unterauftragnehmer unmittelbar gegenüber dem Auftraggeber dieselben Verpflichtungen übernehmen, die dem Auftragnehmer gemäß dieser ADV obliegen. Der Auftragnehmer haftet für das Handeln von Unterauftragnehmern wie für eigenes Handeln. Die Verträge sind auf Wunsch dem Auftraggeber in Kopie zu übergeben. Die mit den Unterauftragnehmern ausgehandelten Preise können geschwärzt werden.

(3) Der Abschluss von neuen Verträgen mit den aufgezählten oder anderen Unterauftragnehmern bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

Holt der Auftragnehmer die erforderliche vorherige Zustimmung des Auftraggebers nicht ein und schließt gleichwohl einen neuen Vertrag mit einem Unterauftragnehmer, berechtigt dies den Auftraggeber zur außerordentlichen Kündigung des Vertrags mit dem Auftragnehmer.

(4) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungspersonal, Wirtschaftsprüfung oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7
Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die nach § 11 Absatz 3 Satz 3 vorgesehene Überprüfung sowie in Nr. 6 der Anlage zu § 9 Absatz 1 Satz 1 DSG-EKD vorgesehene Auftragskontrolle durchzuführen oder durch im Einzelfall zu benennende Personen durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Absatz 3 Satz 3 DSG-EKD und im Wege der Vorabkontrolle nach § 21 Absatz 3 DSG-EKD stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 Absatz 1 DSG-EKD und der Anlage 1 dieses Vertrages nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfung, Revision, Compliance-Beauftragte(r), Datenschutzbeauftragte(r), IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit, z. B. nach BSI-Grundschutz) erbracht werden.

(3) Die Prüfungs-, Zutritts- und Auskunftsrechte stehen auch der oder dem Beauftragten für den Datenschutz der EKD zu.

§ 8
Informations- und Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich zu benachrichtigen, wenn der Verdacht besteht, dass der Auftragnehmer, seine Unterauftragnehmer oder die bei ihm oder seinen Unterauftragnehmern beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die in dieser ADV getroffenen Festlegungen verstoßen haben bzw. verstoßen. Die Informationsverpflichtung des Auftragnehmers besteht auch bei schwerwiegenden Betriebsstörungen, bei Verstößen gegen die in dieser Vereinbarung getroffenen Festlegungen (dazu gehören auch vertragsrelevante technische oder organisatorische Störungen) oder anderen Unregelmäßigkeiten bei der Erhebung, Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers.

Im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von Daten durch Dritte behält sich der Auftraggeber das Recht vor, die Betroffenen und Dritte zu benachrichtigen. In diesem Fall informiert der Auftragnehmer unverzüglich den Auftraggeber und unterstützt ihn kostenfrei bei der Erfüllung derartiger Benachrichtigungen.

Der Auftragnehmer hat in diesen Fällen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Der Auftraggeber ist über die getroffenen Maßnahmen zu informieren.

(2) Über Maßnahmen von Strafverfolgungsorganen [oder von Aufsichtsbehörden nach § 38 Absatz 5 BDSG sowie über Ermittlungsmaßnahmen nach §§ 43, 44 BDSG] wird der Auftragnehmer den Auftraggeber unaufgefordert unverzüglich in Kenntnis setzen, sofern hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist oder sein kann.

(3) Über Kontrollen und Maßnahmen der oder des staatlichen Datenschutzbeauftragten oder der oder des Beauftragten für den Datenschutz der EKD wird der Auftragnehmer den Auftraggeber unaufgefordert unverzüglich in Kenntnis setzen, sofern hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist.

§ 9
Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Der Auftragnehmer wird die Weisungen des Auftraggebers beachten und befolgen und einer ihm angemessenen Nachkontrolle auf Richtigkeit und Plausibilität unterziehen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform (§ 126b BGB) bestätigen.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften oder gegen diese

ADV. Der Auftragnehmer ist berechtigt, die Durchführung einer Weisung, die seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt, so lange auszusetzen, bis diese durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird. Über seine Bedenken hat er den Auftraggeber unverzüglich zu informieren.

(4) Zur Erteilung und zum Empfang von Weisungen betreffend die Auftragsdatenverarbeitung sind ausschließlich die in Anlage 2 genannten Personen berechtigt. Jede Partei ist berechtigt, die Benennung berechtigter Personen jederzeit durch schriftlich Mitteilung gegenüber der jeweils anderen Partei mit einer Ankündigungsfrist von zwei Wochen zu ändern. Bei einem Wechsel oder einer dauerhaften Verhinderung einer benannten Person ist dies der anderen Partei unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen.

§ 10
Löschung von Daten und Rückgabe von Datenträgern, Dokumentation

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens jedoch mit der Beendigung des Hauptvertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie für Test- und Ausschussmaterial. Das zur Datenlöschung anzuwendende Löschverfahren wird in der Anlage 1 näher beschrieben. Die Löschung der Daten ist zu protokollieren, und das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend den jeweiligen gesetzlichen oder zwischen den Parteien vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11
Formklausel

Änderungen und Ergänzungen dieser ADV, der mit Bezug hierauf zwischen den Parteien getroffenen weiteren Vereinbarungen sowie alle unmittelbar den Inhalt oder den Umfang der von den Parteien unter diesem Vertrag geschuldeten Leistungen ändernden oder sonst beeinflussenden Erklärungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 12
Salvatorische Klausel mit Ersetzungsklausel

Sollte eine der Regelungen dieser ADV oder einer mit Bezug hierauf geschlossener weiteren Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden oder diese ADV eine nach übereinstimmender Auffassung der Parteien regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Anstelle der unwirksamen Regelung oder in Ausfüllung der Lücke gelten die gesetzlichen Bestimmungen.

Für den Auftraggeber: Für den Auftragnehmer:

(Ort, Datum)	(Ort, Datum)
(Unterschriften mit Amts- / Funktionsbezeichnungen)	(Unterschriften mit Amts- / Funktionsbezeichnungen)

Anlagen: 2

B. Anlage 1: Hinweise zur Erstellung einer Anlage zur ADV nach § 11 DSG-EKD

Datenschutzkonzept nach der Anlage zu § 9 Abs. 1 DSG-EKD des **Name des Auftragnehmers**	Die Anlage „Datenschutzkonzept“ orientiert sich im Wesentlichen an den Anforderungen der Anlage zu § 9 Abs. 1 DSG-EKD. Die Anlage zu § 9 Abs. 1 DSG-EKD ist wiederum inhaltsgleich zu Anlage zu § 9 BDSG. Alle tatsächlich beim *Auftragnehmer* ergriffenen technischen und organisatorischen Maßnahmen sind anzugeben. Ist ein IT-Sicherheitskonzept vorhanden können die Angaben zu den technischen und organisatorischen Maßnahmen in das Datenschutzkonzept übernommen werden.
Name des Auftragnehmers hat zum Schutz personenbezogener Daten des **Names des Auftraggebers** bei der Auftragsdatenverarbeitung das nachfolgende Datenschutzkonzept erstellt:	
Technische und organisatorische Maßnahmen Name des Auftragnehmers hat gemäß § 9 Abs. 1 DSG-EKD und der dazugehörigen Anlage die folgenden technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ergriffen:	
1. Zutrittskontrolle Maßnahmen, die Unbefugten den räumlichen Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 1 der Anlage zu § 9 Abs. 1 DSG-EKD. Z. B. Schlüsselregelung durch Ausweise, Schlüssel, Magnet- oder Chipkarten (beachte: § 7b DSG-EKD), Tür-, Fenstersicherungen, Alarmanlagen, unterschiedliche Sicherheitszonen, Sicherheitsdienst, Personenkontrolle durch Pförtner, Überwachungseinrichtungen wie Alarmanlagen, Videokameras etc. (beachte: § 7b DSG-EKD), Protokollierung der ein- und ausgehenden Personen, Gehäuseversiegelung von

	technischen Geräten, Regelungen für Reinigung, Wartung, Reparatur, Besucher.
2. Zugangskontrolle Maßnahmen, die verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können. Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 2 der Anlage zu § 9 Abs. 1 DSG-EKD. Eine Maßnahme nach Satz 2 Nr. 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Z. B. Einrichtung (nur) eines Benutzerkontos pro Person, Passwortschutz (einschließlich Mindestanforderungen und Anweisung an das Personal zum Umgang mit Passwörtern), enge Begrenzung der befugten Benutzer, automatische Sperrungen angemeldeter Arbeitsplätze, Verschlüsselung von Datenträgern, Protokollierung der Benutzung und Missbrauchsversuche einschließlich regelmäßiger Auswertung der Protokolle, Verschlüsselung für die Übertragung von Passwörtern, Einsatz eines VPN, spezielle Sicherheitssoftware, Firewall.
3. Zugriffskontrolle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 3 der Anlage zu § 9 Abs. 1 DSG-EKD. Eine Maßnahme nach Satz 2 Nr. 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Z. B. Berechtigungssysteme, Berechtigungsmanagement, Vergabe von Berechtigungen nur im Umfang des Bedarfs, Aktivitäten- und Zugriffsprotokollierungen, gesicherte Archivierung von Daten, Verschlüsselung der Festplatte oder von Partitionen, Zugriffsschutz der Serverplatten.
4.Weitergabekontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Vgl. Satz 2 Nr. 4 der Anlage zu § 9 Abs. 1 DSG-EKD. Eine Maßnahme nach Satz 2 Nr. 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Klicken Sie hier, um Text einzugeben.	Z. B.. separate Kommunikationswege bei der Übermittlung von Passwörtern oder ähnlich sensitiven Daten, Verschlüsselung des Datenbestands, Verschlüsselung bei Übermittlung (sog. Transportverschlüsselung mittels SSL/TLS), sichere Verbindungen (VPN etc.), Signaturverfahren, Protokollierungen, geprüfte Zuverlässigkeit des Spediteurs, Sicherheit von Transportbehältern, Begleitpapiere, Identitätsnachweise des Empfängers, Protokollierung der Abruf- und Übermittlungsaktivitäten.
5.Eingabekontrolle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 5 der Anlage zu § 9 Abs. 1 DSG-EKD. Z. B. Datenerfassungsanweisungen, automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung, der Administrator-Aktivitäten, Protokollauswertungsverfahren für Datenzugriffe, Freigabeverfahren und Dokumentation der aktuellen Programmversionen, Plausibilitätskontrollen.
6. Auftragskontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. (*Beachte: Das zur Datenlöschung anzuwendende Löschverfahren nach § 10 Abs. 1 dieses Vertrages ist näher zu beschreiben.)* Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 6 der Anlage zu § 9 Abs. 1 DSG-EKD. Z. B. Arbeitsvertragsgestaltung mit Mitarbeitern, Erlass entsprechender Arbeits- bzw. Dienstanweisungen, Auswahlverfahren bei Unterauftragnehmern, formalisierte Auftragserteilungen, regelmäßige Ausübung von Kontrollbefugnissen gegenüber Mitarbeitern bzw. Unterauftragnehmern einschließlich konsequenter Durchsetzung mittels Sanktionen, Verpflichtung des Personals auf das Datengeheimnis (§ 6 DSG-EKD), Datenübergabe nur gegen Quittung oder verschlüsselt, Prüfung der Identitäten des Personals des Auftraggebers.
7. Verfügbarkeitskontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Vgl. Satz 2 Nr. 7 der Anlage zu § 9 Abs. 1 DSG-EKD. Z. B. Lagerbedingungen von

Klicken Sie hier, um Text einzugeben.	Sicherheitskopien, unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Back-up- und Wiederanlauf- und Katastrophenfallkonzepte (einschließlich Zielvorgaben für Wiederanlaufzeit und Grad der Wiederherstellung), Tresore.
8. Trennungskontrolle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, z. B. Erfassung, Zuordnung und Berücksichtigung eines Zwecks zu jedem Datum, Funktionstrennung Klicken Sie hier, um Text einzugeben.	Vgl. Satz 2 Nr. 8 der Anlage zu § 9 Abs. 1 DSG-EKD. Z. B. Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken, Zugriff auf Datensätze nur über zuvor festgelegte Programme, Erfassung, Zuordnung und Berücksichtigung eines Zwecks zu jedem Datum, Funktionstrennung (Test-, Produktivumgebung), „Mandantenfähigkeit“ der Software.

C. Anlage 2: Berechtigte Weisungsgeber und Weisungsempfänger, Datenschutzbeauftragte

Zur Erteilung von Weisungen betreffend die Auftragsdatenverarbeitung sind aufseiten des Auftraggebers folgende Personen[1] berechtigt:

Klicken Sie hier, um Text einzugeben.
(Name, Funktion, Anschrift, Telefon, Fax, E-Mail)

Zum Empfang von Weisungen betreffend die Auftragsdatenverarbeitung sind aufseiten des Auftragnehmers ausschließlich folgende Personen berechtigt:

Klicken Sie hier, um Text einzugeben.
(Name, Funktion, Anschrift, Telefon, Fax, E-Mail)

Beim Auftragnehmer ist folgende Person

[Name und Kontaktdaten]

☐ als örtlich Beauftragte(r) für den Datenschutz bestellt.

☐ als Betriebsbeauftragte(r) für den Datenschutz bestellt.

☐ als Beauftragte(r) für den Datenschutz bestellt (siehe §§ 4f, 4g BDSG).

Beim Auftraggeber ist folgende Person

[Name und Kontaktdaten]

☐ als örtlich Beauftragte(r) für den Datenschutz bestellt.

☐ als Betriebsbeauftragte(r) für den Datenschutz bestellt.

[1] Ggf. auch die oder den örtlich Beauftragte(n) oder die oder den Betriebsbeauftragte(n) für den Datenschutz als weisungsberechtigte Person aufnehmen.

D. Erläuterungen / Ausfüllhinweise zur Arbeitshilfe zur Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11 Datenschutzgesetz-EKD

Die Auftragsdatenverarbeitung muss im Rahmen der für den Auftraggeber geltenden Vorschriften abgewickelt werden (Datenschutzgesetz-EKD, Datenschutzdurchführungsverordnungen der EKD und der Gliedkirchen u. a.). Bei einer Auftragsdatenverarbeitung ist nicht der Auftragnehmer für die Einhaltung der kirchlichen Datenschutzvorschriften verantwortlich, diese Verantwortlichkeit verbleibt beim Auftraggeber. Der Auftraggeber ist verpflichtet, den Auftragnehmer sorgfältig auszuwählen, und er hat sich selber von der Einhaltung der Datenschutzvorschriften zu überzeugen. Der Auftragnehmer muss seinerseits intern sicherstellen, dass die Datenerhebung, -verarbeitung und -nutzung nur nach den durch den Auftraggeber festgelegten Weisungen erfolgt und die technischen und organisatorischen Maßnahmen eingehalten werden.

Dessen ungeachtet muss der Auftragnehmer, soweit es sich um eine nichtkirchliche Stelle handelt, die Vorschriften des Bundesdatenschutzgesetzes (BDSG) beachten, wenn der Auftragnehmer fremde Daten im Auftrag erhebt, verarbeitet oder nutzt (Datengeheimnis § 5 BDSG, Datensicherungsmaßnahmen einschließlich Trennungsgebot § 9 BDSG, Strafvorschrift § 44 BDSG, Ordnungswidrigkeiten § 43 BDSG).

Zur Präambel

Die Angaben der Präambel sind ggf. bei der Auslegung der weiteren Regelungen in dieser Vereinbarung heranzuziehen.

In dem Hauptvertrag sind u. a. Regelungen zur Laufzeit, Vergütung, Kündigung, Schadenersatz, Vertragsstrafe, Haftung, anwendbares Recht, Gerichtsstand aufzunehmen. Der Hauptvertrag wird in aller Regel ein Dienst- oder Werkvertrag sein, der die vom Auftragnehmer zu erbringenden Leistungen beschreibt. Der Hauptvertrag und die in diesem enthaltene Leistungsbeschreibung stellen die Grundlage für die Weisungen des Auftraggebers dar. Im Rahmen der Vergütung ist zu regeln, dass die Kosten für das Datenschutz- und IT-Sicherheitskonzept vom Auftragnehmer zu tragen sind.

Der Auftraggeber als „Herr der Daten“ hat in seiner Auftragserteilung zu regeln, wie die Verarbeitung der personenbezogenen Daten erfolgen soll, wie dies organisatorisch abläuft, welche Datensicherheitsmaßnahmen erforderlich sind und wie einzelne Vorgaben technisch umgesetzt werden sollen. Bereits bei der Auswahl eines geeigneten Auftragnehmers ist auf die Einhaltung der Vorgaben zu achten. In der Praxis werden viele der geforderten Vorgaben bereits umgesetzt sein. Kann ein potenzieller Auftragnehmer diese Vorgaben nicht umsetzen, kann eine Datenverarbeitung im Auftrag mit ihm nicht vereinbart werden.

Zu § 1 Abs. 1

Siehe auch § 11 Absatz 3 Satz 2 Ziffer 1 DSG-EKD. Soweit der Gegenstand und Dauer des Auftrags mit denen des jeweiligen Hauptvertrags (z. B. Rahmenvertrag, Leistungsschein, Einzelauftrag) identisch sind, kann unter § 1 Absatz 1 auf die jeweilige Stelle im Hauptvertrag verwiesen werden (z. B. Gegenstand: „Der Gegenstand des Auftrags ergibt sich aus § XY Hauptvertrag“).

Zu § 1 Abs. 3

Neben den Absätzen 1 und 2 ist bei Auftragsdatenverarbeitungen, die die (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen betreffen, Absatz 3 zusätzlich aufzunehmen.

In der Praxis kann bei vielen Dienstleistungen der IT-Branche (Installation und Wartung von Netzwerken, Hardware [incl. Telekommunikationsanlagen] sowie Pflege von Software u. a. [Betriebssysteme, Anwendungen], Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests, Durchführung von Migrationen im Produktivsystem, Parametrisieren von Software) ein ggf. unbeabsichtigtes Kenntnisnehmen personenbezogener Daten des Auftragnehmers erfolgen.

Das DSG-EKD ordnet lediglich die „entsprechende“ Anwendung der Vorschriften zur Auftragsdatenverarbeitung an. Bei der Anwendung der Vorschriften müssen etwaige Besonderheiten, die für die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen charakteristisch sind, Berücksichtigung finden. Dabei ist es unerheblich, ob die Wartungsmaßnahmen vor Ort oder per Fernwartung durchgeführt werden (Remote-Zugriff des Auftragnehmers auf personenbezogene Daten beim Auftraggeber).

Zu § 2 Abs. 2

Siehe auch § 11 Absatz 3 Satz 2 Ziffer 2 DSG-EKD. Die Festlegungen haben unmittelbare Auswirkungen auf die Rechtmäßigkeit des Datenumgangs durch den Auftragnehmer; sie sollen eindeutig und vollständig aufgeführt werden.

Zu § 3

Nach § 11 Absatz 3 Satz 2 Ziffer 3 DSG-EKD sind zwingend Angaben zu den vereinbarten technische und organisatorische Maßnahmen nach § 9 Abs. 1 DSG-EKD und seiner Anlage in die ADV aufzunehmen. Es ist erforderlich, z. B. den gesamten Ablauf vom Transport der Daten über die Festlegung der Zugriffsrechte bis zur Löschung der Daten in einer gesonderten Anlage 1 (dem Datenschutz- oder IT-Sicherheitskonzept) darzustellen. Die schriftliche Fixierung hilft dem Auftraggeber, seine Kontrollrechte effektiv wahrnehmen zu können.

Sollte die Vereinbarung mit kirchlichen Stellen abgeschlossen werden, kann von einer Auflistung der technischen und organisatorischen Sicherheitsmaßnahmen (Datenschutzkonzept) nach Anlage 1 sowie von der Vorlage eines IT-Sicherheitskonzeptes abgesehen werden. Dies ist insbesondere dann der Fall, wenn Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz gemäß § 22 DSG-EKD bestellt sind. Durch Kontaktaufnahme mit der oder dem Betriebsbeauftragten bzw. örtlich Beauftragten für den Datenschutz und ggf. im Rahmen einer Ortsbesichtigung kann sich der Auftraggeber einen Überblick über die vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen verschaffen. Im Einzelfall können Absatz 1 Satz 3, Absatz 2 und 3 der Arbeitshilfe entbehrlich sein.

Zu § 3 Abs. 2 Satz 3

Bei der Verarbeitung personenbezogener Daten ist vom Auftraggeber der Schutzbedarf festzulegen. Bei einem mittleren oder hohen Schutzbedarf der personenbezogenen Daten ist ein IT-Sicherheitskonzept vorzulegen. In anderen Fällen, insbesondere wenn der Schutzbedarf der personenbezogenen Daten als einfach eingestuft ist, kann im Einzelfall von der Übergabe des IT-Sicherheitskonzeptes abgesehen werden. In diesen Fällen kann Abs. 2 Satz 3 der Vereinbarung gestrichen werden. Dabei wird vorausgesetzt, dass angemessene Schutzmaßnahmen nach der Anlage 1 dieser Vereinbarung realisiert sind.

Zu § 3 Abs. 4

Nr. 8 der Anlage zu § 9 Absatz 1 Satz 1 DSG-EKD sieht vor, dass insbesondere Maßnahmen zu treffen sind, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle). Die logische Datentrennung von Daten Dritter ist auch zwingender Bestandteil der Anlage 1 (Daten- oder IT-Sicherheitskonzept). Zulässige Maßnahmen können z. B. softwareseitiger Ausschluss (Mandantentrennung), Dateiseparierung bei Datenbankprinzip, Trennung über Zugriffsregelung, Trennung von Test- und Routineprogrammen sein.

Zu § 4

Siehe auch § 11 Absatz 3 Satz 2 Ziffer 4 DSG-EKD.

Zu § 4 Abs. 1

Wegen der Löschung von Daten kann es im Einzelfall erforderlich sein, Löschfristen und die Verfahrensabläufe bei der Löschung detailliert festzulegen. Folgender Alternativvorschlag ist auch möglich:

„(1) Wird festgestellt, dass Daten unrichtig sind, hat sie der Auftragnehmer nach Abstimmung mit dem Auftraggeber unverzüglich zu berichtigen. Für das laufende Verfahren nicht mehr benötigte Daten sind zu löschen; sie sind zu sperren, wenn gesetzliche Aufbewahrungs- oder Archivierungspflichten bestehen.“

Zu § 4 Abs. 2

Bei der Auftragsdatenverarbeitung bleibt der Auftraggeber Adressat der Ansprüche von betroffenen Personen, die ihre Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung geltend machen können.

Zu § 5 Abs. 1 Satz 2

Die Verpflichtung der Mitarbeitenden auf das Datengeheimnis ist zwingend, sofern der Auftragnehmer eine nichtkirchliche Stelle (in der Regel aus der Privatwirtschaft) ist. Bei beauftragten kirchlichen Stellen entfällt die Schriftform der Verpflichtung nach § 6 Satz 2 DSG-EKD, wenn die Mitarbeitenden des Auftragnehmers auf Grund anderer kirchlicher arbeits- oder beamtenrechtlicher Bestimmungen zur Verschwiegenheit verpflichtet sind. Für die Verpflichtung der Beschäftigten des Auftragnehmers ist das Formblatt nach den jeweiligen Durchführungsbestimmungen zu verwenden.

Zu § 5 Abs. 4

Siehe auch § 11 Absatz 5 DSG-EKD. Dieser Absatz kann entfallen, sofern es sich bei dem Auftragnehmer um eine kirchliche Stelle handelt.

Zu § 5 Abs. 6

Aus der Vorgabe der Vereinbarung ergibt sich, dass die Auftragsdatenverarbeitung vorrangig in Deutschland stattfinden soll. Dies ist dadurch begründet, dass in Deutschland ein hohes Datenschutzniveau vorhanden ist und eine Kontrolle des Auftragnehmers vor Ort erleichtert wird. Das DSG-EKD lässt eine Auftragsdatenverarbeitung grundsätzlich auch außerhalb Deutschlands zu. Nach § 11 Absatz 2 DSG-EKD darf die beauftragte Stelle die Daten nur innerhalb der Mitgliedsstaaten der Europäischen Union erheben, verarbeiten oder nutzen. Die Evangelische Kirche in Deutschland kann die Datenerhebung, -verarbeitung und -nutzung in Staaten außerhalb der Europäischen Union zulassen, wenn diese ein dem EKD-Datenschutzgesetz angemessenes gesetzliches oder vertraglich vereinbartes Datenschutzniveau nachgewiesen haben. Für den Fall der Datenverarbeitung in einem Mitgliedsstaat der Europäischen Union ist zu beachten, dass grenzüberschreitende Auftragsdatenverarbeitungen ebenso in die vom Auftraggeber regelmäßig durchzuführenden Kontrollen einzubeziehen sind. Der Auftraggeber kann es zulassen, dass der Auftragnehmer seiner Kontrollverpflichtung auch auf andere Weise nachkommt (z. B. Einschaltung von sachverständigen Dritten, Fragebögen, Anforderung von Prüfdokumentationen oder Zertifikaten). Findet die Auftragsdatenverarbeitung in einem Mitgliedsstaat der EU statt, wäre dies im § 5 Abs. 6 Satz 1 zu konkretisieren.

Zu § 5 Abs. 7

Näheres ist im Datenschutzkonzept in der Anlage 1 zu regeln. In der Regel sollen die Daten verschlüsselt werden.

Zu § 5 Abs. 8

In dem jeweiligen Ausnahmefall sollte sich der Auftraggeber die zwischen dem Auftragnehmer und seinem Beschäftigten abgeschlossene Vereinbarung vorlegen lassen. Im Rahmen der Überprüfung sind der Arbeitsplatz des Beschäftigten und die festgelegten technischen und organisatorischen Maßnahmen einzubeziehen.

Zu § 6

Für einzelne Tätigkeitsbereiche der Datenerhebung, -verarbeitung oder -nutzung kann es notwendig sein, Unterauftragnehmer einzusetzen. Zwischen Auftraggeber und Auftragnehmer ist daher die Zulässigkeit oder Nichtzulässigkeit bestehender und zukünftiger Unterauftragsverhältnisse zu regeln.

Zu § 6 Abs. 3

Hierzu zählen alle Vertragsänderungen. Es kann vereinbart werden, dass Vertragsänderungen ausgenommen sind, die sich ausschließlich in der Vereinbarung neuer Preise erschöpfen.

Zu § 7

Die kirchliche Stelle bleibt gegenüber den Betroffenen nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung. Um das Haftungsrisiko gegenüber den Betroffenen zu minimieren, muss die kirchliche Stelle als Auftraggeber sich jederzeit, auch nach Beginn der Datenverarbeitung, von der ordnungsgemäßen Vertragsdurchführung durch den Auftragnehmer überzeugen zu können. Es ist nicht erforderlich, dass sich der Auftraggeber unmittelbar beim

Auftragnehmer vor Ort oder selbst in Person überzeugt. Je nach Einzelfall kann der Nachweis auch anderweitig erbracht werden (siehe § 7 Absatz 2).

Zu § 7 Abs. 1

Für den Auftraggeber können entsprechend qualifizierte Personen tätig werden (z. B. die oder der örtlich Beauftragte oder Betriebsbeauftragte für den Datenschutz). Diese Person nimmt beim Auftragnehmer die Erstkontrolle und die regelmäßigen Kontrollen vor.

Zu § 7 Abs. 2

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig (z. B. im Rhythmus von ein oder zwei Jahren) von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Im Rahmen der Kontrolle sind die in der Anlage aufgeführten Maßnahmen zu begutachten. Bei nichtkirchlichen Stellen gehört zur Überprüfung z.B. auch das Vorlegen der Verpflichtungserklärungen der Mitarbeitenden des Auftragnehmers auf das Datengeheimnis. Die Kontrolle hat sich auch auf Unterauftragnehmer zu erstrecken. Die Überprüfung kann vor Ort erfolgen, oder es können auch die von Dritten durchgeführten Begutachtungen akzeptiert werden, wenn entsprechende Nachweise vorgelegt werden. Bei kirchlichen Stellen als Auftragnehmer sind im Einzelfall die Absätze 2 und 3 entbehrlich.

Zu § 8

Siehe auch § 11 Absatz 3 Satz 2 Ziffer 8 DSG-EKD. Da die kirchliche Stelle gegenüber dem Betroffenen nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung bleibt, muss sie über alle Fehlhandlungen, Störungen oder Unregelmäßigkeiten informiert werden.

Zu § 8 Abs. 2

Der Klammertext ist nur aufzunehmen, sofern der Auftragnehmer als nichtkirchliche Stelle nicht dem DSG-EKD sondern dem BDSG unterliegt.

Zu § 8 Abs. 3

Bei einer kirchlichen Stelle nach § 1 Abs. 2 DSG-EKD kann der Hinweis auf den „staatlichen Datenschutzbeauftragten“ entfallen.

Zu § 9

Siehe auch § 11 Absatz 3 Satz 2 Ziffer 9 DSG-EKD und § 11 Absatz 4 Satz 1 DSG-EKD. Die Weisungsgebundenheit ist wesentliches Merkmal der Auftragsdatenverarbeitung. Weisungen können generell oder im Einzelfall erteilt werden.

Zu § 9 Abs. 2

§ 126b BGB erlaubt eine schriftliche Erklärung ohne eigenhändige Unterschrift oder qualifizierte elektronische Signatur. Dadurch wird der Einsatz neuer Techniken (Fax, Computerfax, E-Mail) ermöglicht.

Zu § 9 Abs. 3

Die Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung.

Zu § 10

Der Auftragnehmer muss technisch in der Lage sein, die vertraglich vereinbarte Löschung datenschutzkonform umzusetzen.

Zu § 10 Abs. 1

Es empfiehlt sich, die Maßnahmen zur Vernichtung der Papierdokumente der Datenträger konkret festzulegen. Die erforderlichen Maßnahmen richten sich nach den jeweils aktuellen DIN-Normen sowie dem Maßnahmenkatalog des BSI. Sofern keine Beschreibung in der Anlage 1 dieser Vereinbarung erfolgt, wäre ggf. folgender Textvorschlag aufzunehmen: *„Nach Aufforderung des Auftraggebers werden zu vernichtende Papierdokumente mit personenbezogenen Daten vom Auftragnehmer ordnungsgemäß nach Maßgabe der jeweils aktuellen DIN 66399, Sicherheitsstufe 3 bis 7, entsorgt.*

Das Löschen von Datenträgern erfolgt, sofern der Datenträger hierbei vernichtet werden muss, durch Schreddern oder Zerfasern nach Maßgabe der jeweils aktuellen DIN 66399. Dies gilt auch für bei der Datenverarbeitung durch den Auftragnehmer entstandene Zwischendaten, Arbeitsdateien und sonstiges Ausschussmaterial. Der Auftraggeber ist berechtigt, die Vernichtung bzw. Löschung personenbezogener Daten beim Auftragnehmer zu überwachen.“