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

Die Auftragsdatenverarbeitung muss im Rahmen der für den Auftraggeber geltenden Vorschriften abgewickelt werden (DSG-EKD, DSAG, DATVO, VV-DS). 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).

Zu den Einzelheiten der Vereinbarung:

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.“