Erläuterungen / Ausfüllhinweise zur Arbeitshilfe zur Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 30 Datenschutzgesetz-EKD

Die Auftragsverarbeitung muss unter Beachtung und Umsetzung der für den Auftraggeber geltenden Vorschriften abgewickelt werden (Datenschutzgesetz-EKD, Datenschutzdurchführungsverordnungen der EKD und der Gliedkirchen u. a.). Bei einer Auftragsverarbeitung ist nicht der Auftragsverarbeiter für die Einhaltung der kirchlichen Datenschutzvorschriften verantwortlich. Da der Auftragsverarbeiter datenschutzrechtlich wie eine organisatorische Einheit des Auftraggebers und nicht als Dritter behandelt wird, verbleibt auch die Verantwortlichkeit beim Auftraggeber. Sie ist insb. verpflichtet, den Auftragsverarbeiter sorgfältig auszuwählen und sich durch Kontrollen von der Einhaltung der Datenschutzvorschriften durch den Auftragsverarbeiter zu überzeugen. Der Auftragsverarbeiter muss seinerseits intern sicherstellen, dass die Datenerhebung, -verarbeitung und -nutzung nur nach den durch den Auftraggeber festgelegten Weisungen erfolgt und die notwendigen technischen und organisatorischen Maßnahmen zu treffen.

Zur Präambel

Die Angaben in der Präambel sind vor allem für die Auslegung der weiteren Regelungen des AVV relevant.

Beim Hauptvertrag handelt es sich in der Regel um einen Dienst- oder Werkvertrag, der insb. die vom Auftragsverarbeiter zu erbringenden Leistungen festlegt. Darüber hinaus können – je nach Einzelfall – z. B. Regelungen zu den Themen Vergütung, Laufzeit, Kündigung, Schadenersatz, Vertragsstrafe, Haftung, anwendbares Recht und Gerichtsstand aufgenommen werden. In der Vergütungsregelung des Hauptvertrags sollte insbesondere bestimmt werden, dass die Kosten für das Datenschutz- und IT-Sicherheitskonzept vom Auftragsverarbeiter zu tragen sind. Der Hauptvertrag und die in ihm enthaltene Leistungsbeschreibung stellen die Grundlage für die Weisungen des Auftraggebers dar.

Der Auftraggeber hat als „Herrin der Daten“ bereits bei Auftragserteilung durch den AVV zu regeln, wie die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter erfolgen soll, wie dies organisatorisch abläuft, welche Datensicherheitsmaßnahmen erforderlich sind und wie einzelne Vorgaben technisch umgesetzt werden sollen. Bereits bei der Auswahl eines geeigneten Auftragsverarbeiters ist auf die Einhaltung der Vorgaben zu achten. In der Praxis werden viele dieser Anforderungen Vorgaben bereits umgesetzt sein. Kann ein potenzieller Auftragsverarbeiter diese Vorgaben nicht umsetzen, kommt er für die Durchführung einer Auftragsverarbeitung im Sinne des § 30 DSG-EKD nicht in Betracht.

Zu § 1 Absatz 1 und 2

Siehe auch § 30 Absatz 3 Satz 2 Nummer 1 DSG-EKD. Soweit Gegenstand und Dauer der Auftragsverarbeitung mit denen des jeweiligen Hauptvertrags identisch sind, kann unter § 1 Absatz 1 auf die relevante Stelle im Hauptvertrag verwiesen werden (z. B. „Der Gegenstand des Auftrags ergibt sich aus § 2 Absatz 1 bis 3 des Hauptvertrags“). Der Verweis sollte zur eindeutigen Bestimmung der Vertragsinhalte so konkret wie möglich gestaltet und der Hauptvertrag als Anhang zum vorliegenden AVV geführt werden.

Bedeutsam für den AVV ist vor allem die Laufzeitregelung des Hauptvertrags da § 1 Absatz 2 auf diese verweist.

Auch für Aufträge, welche die (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen betreffen, muss nach § 30 Absatz 6 DSG-EKD ein AVV abgeschlossen werden, wenn bei Durchführung des Auftrags ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. In der Praxis kann es bei vielen Dienstleistungen der IT-Branche zu einer ggf. unbeabsichtigten Kenntnisnahme personenbezogener Daten durch den Auftragsverarbeiter kommen. Hierbei ist etwa an die Installation und Wartung von Netzwerken und Hardware (incl. Telekommunikationsanlagen) sowie die Pflege von Software (z. B. Betriebssysteme, Anwendungen), Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests, Durchführung von Migrationen im Produktivsystem und das Parametrisieren von Software zu denken.

Bei der entsprechenden Anwendung von § 30 Absatz 1 bis 5 DSG-EKD sind etwaige Besonderheiten, die für die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen charakteristisch sind, zu berücksichtigen. Dabei ist es unerheblich, ob die Wartungsmaßnahmen vor Ort oder per Fernwartung als Remote-Zugriff des Auftragsverarbeiters auf personenbezogene Daten bei dem Auftraggeber durchgeführt werden.

Zu § 2 Absatz 2

Siehe auch § 30 Absatz 3 Satz 2 Nummer 2 DSG-EKD. Die Festlegungen haben unmittelbare Auswirkungen auf die Rechtmäßigkeit des Datenumgangs durch den Auftragsverarbeiter. Sie sollen eindeutig und vollständig aufgeführt werden.

Soweit zur Bestimmung von Umfang, Art und Zweck der Datenverarbeitung auf separate Dokumente verwiesen wird, sollten die einschlägigen Textabschnitte möglichst genau benannt werden, z. B. durch Verweis auf konkrete Paragraphen des Hauptvertrags. Darüber hinaus sollten sie jeweiligen Dokumente als Anlage zum AVV geführt werden.

Zu § 3

Nach § 30 Absatz 3 Satz 2 Nummer 3 DSG-EKD sind zwingend Angaben zu den vereinbarten technischen und organisatorischen Maßnahmen nach § 27 DSG-EKD in den AVV aufzunehmen. Zur Umsetzung dieser Pflicht ist insbesondere der gesamte Ablauf vom Transport der Daten über die Festlegung der Zugriffsrechte bis zur Löschung der Daten in der gesonderten Anlage 1 darzustellen. In vielen Fällen können hierbei bereits bestehende Datenschutz- und IT-Sicherheitskonzepte Orientierungszwecken herangezogen werden. Die schriftliche Fixierung hilft dem Auftraggeber, zum einen bei effektiven der Wahrnehmung ihrer Kontrollrechte gegenüber dem Auftragsverarbeiter. Zum anderen kann sie vom Auftraggeber herangezogen werden, um ihrer Nachweispflicht aus § 5 Absatz 2 DSG-EKD nachzukommen.

Zu § 3 Absatz 1 Satz 5

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 Absatz 1 Satz 5 der Vereinbarung gestrichen werden. Dabei wird vorausgesetzt, dass angemessene Schutzmaßnahmen nach der Anlage 1 dieser Vereinbarung realisiert sind.

Zu § 3 Absatz 5

Die logische Datentrennung von Daten Dritter ist auch zwingender Bestandteil der Anlage 1. Zulässige Maßnahmen können z. B. softwareseitiger Ausschluss (Mandantentrennung), Datei-

separierung bei Datenbankprinzip, Trennung über Zugriffsregelung, Trennung von Test- und Routineprogrammen sein.

Zu § 4

Siehe auch § 30 Absatz 3 Satz 2 Nummer 4 DSG-EKD.

Zu § 4 Absatz 1

Hinsichtlich der Löschung von Daten kann es erforderlich sein, Löschfristen und die Verfahrensabläufe bei der Löschung detailliert festzulegen. Alternativ kann auch die folgende Formulierung verwendet werden:

„(1) Wird festgestellt, dass Daten unrichtig sind, hat sie der Auftragsverarbeiter nach Abstimmung mit dem Auftraggeber unverzüglich zu berichtigen. Die Verarbeitung von für das laufende Verfahren nicht mehr benötigten Daten ist einzuschränken. Gesetzliche Aufbewahrungs- oder Archivierungspflichten sind zu beachten, anderenfalls sind sie zu löschen."

Zu § 4 Absatz 2

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

Zu § 5 Absatz 1 Satz 2

Die Verpflichtung der Mitarbeitenden auf das Datengeheimnis ist zwingend, sofern der Auftragsverarbeiter eine nichtkirchliche Stelle (in der Regel aus der Privatwirtschaft) ist. Bei beauftragten kirchlichen Stellen entfällt die Verpflichtung nach § 26 Satz 2 DSG-EKD, wenn die Mitarbeitenden des Auftragsverarbeiters auf Grund anderer kirchlicher arbeits- oder beamtenrechtlicher Bestimmungen zur Verschwiegenheit verpflichtet sind. Für die Verpflichtung der Beschäftigten des Auftragsverarbeiters ist das Formblatt nach den jeweiligen Durchführungsbestimmungen zu verwenden.

Zu § 5 Absatz 4

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

Zu § 5 Absatz 6

Nachdem mit dem Inkrafttreten der EU-Datenschutz-Grundverordnung in der gesamten Europäischen Union ein einheitlich hohes Datenschutzniveau etabliert wurde, stellt das DSG-EKD an die Auftragsverarbeitung in anderen EU-Mitgliedstaaten dieselben Anforderungen wie an die Auftragsverarbeitung innerhalb Deutschlands. Darüber hinaus ist unter den Voraussetzungen des § 10 DSG-EKD in Verbindung mit § 30 Absatz 2 DSG-EKD auch eine Auftragsverarbeitung außerhalb der Europäischen Union möglich. Jedoch ist für den Fall der Datenverarbeitung in einem anderen EU-Mitgliedsstaat zu berücksichtigen, dass grenzüberschreitende Auftragsverarbeitungen in die vom Auftraggeber regelmäßig durchzuführenden Datenschutzkontrollen einzubeziehen sind. Mit Blick auf Kontrollen am Dienstsitz des Auftragsverarbeiters können dem Auftraggeber daher im Vergleich zur Auftragsverarbeitung innerhalb Deutschlands erhebliche organisatorische und wirtschaftliche Mehraufwände entstehen. Soll die Auftragsdatenverarbeitung außerhalb Deutschlands stattfinden, ist dies in § 5 Absatz 6 Satz 1 zu konkretisieren.

Der Auftraggeber kann es zulassen, dass der Auftragsverarbeiter seinen Kontrollpflichten auch auf andere Wiese nachkommt (z. B. durch Einschaltung von sachverständigen Dritten, Fragebögen oder Anforderung von Prüfdokumentationen oder Zertifikaten).

Zu § 5 Absatz 7

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

Zu § 5 Absatz 8

In dem jeweiligen Ausnahmefall sollte sich der Auftraggeber die zwischen dem Auftragsverarbeiter 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 Datenverarbeitung kann es notwendig sein, Unterauftragnehmer einzusetzen. Zwischen dem Auftraggeber und dem Auftragsverarbeiter ist daher die Zulässigkeit oder Nichtzulässigkeit bestehender und zukünftiger Unterauftragsverhältnisse zu regeln.

Zu § 6 Absatz 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 Personen nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung. Um das Haftungsrisiko gegenüber den betroffenen Personen zu minimieren, muss der Auftraggeber sich jederzeit, auch nach Beginn der Datenverarbeitung, von der ordnungsgemäßen Vertragsdurchführung durch den Auftragsverarbeiter überzeugen zu können. Es ist nicht in jedem Fall erforderlich, dass sich der Auftraggeber hiervon unmittelbar beim Auftragsverarbeiter vor Ort oder selbst in Person überzeugt. Je nach Einzelfall kann der Nachweis auch anderweitig erbracht werden (siehe § 7 Absatz 2).

Zu § 7 Absatz 1

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

Zu § 7 Absatz 2

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig (z. B. im Rhythmus von ein oder zwei Jahren, in Fällen besonderen Anlasses auch häufiger) von der Einhaltung der beim Auftragsverarbeiter 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 Auftragsverarbeiters 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, soweit entsprechende Nachweise vorliegen. Bei kirchlichen Stellen als Auftragsverarbeiter sind im Einzelfall die Absätze 2 und 3 entbehrlich.

Zu § 8

Siehe auch § 30 Absatz 3 Satz 2 Nummer 8 DSG-EKD. Da die kirchliche Stelle gegenüber der betroffenen Person nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung bleibt, muss sie über alle Fehlhandlungen, Störungen oder Unregelmäßigkeiten informiert werden.

Zudem treffen den Auftraggeber und den Auftragsverarbeiter die Meldepflicht aus §§ 32 DSG-EKD. Die dem Auftragsverarbeiter gemäß § 8 aufzuerlegenden Pflichten dürfen keinesfalls hinter den in § 32 Absatz 2 DSG-EKD gesetzlichen Pflichten des Auftragsverarbeiters zurückbleiben. Der Auftraggeber trifft außerdem die Benachrichtigungspflicht aus § 33 DSG-EKD.

Zu § 8 Absatz 2

Der Klammertext ist nur aufzunehmen, sofern der Auftragsverarbeiter als nichtkirchliche Stelle nicht dem DSG-EKD sondern dem staatlichen Datenschutzrecht (EU-Datenschutz-Grundverordnung bzw. Bundesdatenschutzgesetz) unterliegt.

Zu § 8 Absatz 3

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

Zu § 9

Siehe auch § 30 Absatz 3 Satz 2 Nummer 9 DSG-EKD und § 30 Absatz 4 Satz 1 DSG-EKD. Die Weisungsgebundenheit ist wesentliches Merkmal der Auftragsverarbeitung. Weisungen können generell oder im Einzelfall erteilt werden.

Zu § 9 Absatz 2

§ 126 b 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 Absatz 3

Die Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung.

Zu § 10

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

Zu § 10 Absatz 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 Auftragsverarbeiter 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 Auftragsverarbeiter entstandene Zwischendaten, Arbeitsdateien und sonstiges Ausschussmaterial. Der Auftraggeber ist berechtigt, die Vernichtung bzw. Löschung personenbezogener Daten beim Auftragsverarbeiter zu überwachen.“