Anforderungskatalog

zur Bewertung und Zertifizierung von

Auftragsdatenverarbeitungen von Auftragnehmern

für die Zertifizierung

Zertifizierte Auftragsdatenverarbeitung

Version 6.2 | 10.08.2015

TÜV SÜD Sec-IT

Mehr Sicherheit.
Mehr Wert.

Sitz: München
Amtsgericht München HRB 197 698
USt-IdNr. DE282283450
Informationen gemäß § 2 Abs. 1 DL-InfoV
unter www.tuev-sued.de/impressum

Geschäftsführer:
Herbert Huß

Telefon: +49 89 500 84 868
Telefax: +49 89 5155 1097
www.tuev-sued.de

TÜV SÜD Sec-IT GmbH
Ridlerstraße 65
80339 München
Deutschland

2015 © TÜV SÜD Sec-IT GmbH

Inhalte

1 Einführung

Werden personenbezogene Daten im Auftrag erhoben, verarbeitet oder genutzt, bleibt der Auftraggeber für die Einhaltung des Bundesdatenschutzgesetzes und weiterer Vorschriften über den Datenschutz verantwortlich (Auftragsdatenverarbeitung). Der Auftragnehmer ist vom Auftraggeber unter Berücksichtigung der Eignung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz auszuwählen und sodann regelmäßig hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz zu prüfen.[1]

Der Auftraggeber kann selbst diesen Prüfpflichten beim Auftragnehmer nachkommen, sachverständige Dritte mit der Wahrnehmung dieser Prüfpflichten beauftragen oder den Auftragnehmer zur Vorlage geeigneter Zertifikate zum Datenschutz auffordern.

Die Zertifizierung „Zertifizierte Auftragsdatenverarbeitung“ richtet sich in diesem Zusammenhang an Auftragnehmer von Auftragsdatenverarbeitungen und bietet diesen die Möglichkeit, die im Rahmen von Auftragsdatenverarbeitungen eingesetzten Verfahren durch einen sachverständigen und unabhängigen Prüfer (TÜV SÜD Sec-IT GmbH) prüfen und bewerten zu lassen.

Durch Vorlage des Zertifikates „Zertifizierte Auftragsdatenverarbeitung“ kann die Eignung und Angemessenheit der vom Auftragnehmer erstellten leistungs- und auftragsbezogenen Dokumentationen sowie der angewendeten allgemeinen, technischen und organisatorischen Maßnahmen zum Datenschutz hinsichtlich der geprüften und bewerteten Verfahren gegenüber dem Auftraggeber nachgewiesen werden. Dieser Nachweis (Zertifikat) gegenüber dem Auftraggeber kann, wie vom Bundesdatenschutzgesetz für Auftragsdatenverarbeitungen gefordert, bereits bei der Anbahnung von Auftragsvergaben sowie nach Auftragsvergabe fortlaufend erfolgen.

2 Durchführung der Prüfung und Bewertung

Die beim Auftragnehmer zu prüfenden und bewertenden Verfahren sind vor Beginn der Prüfungen und Bewertungen im Einzelnen zu spezifizieren.

Obligatorisch für die Prüfung und Bewertung der im Rahmen von Auftragsdatenverarbeitungen eingesetzten Verfahren ist die Durchführung einer Dokumentenprüfung und eines Audits beim Auftragnehmer vor Ort durch einen sachverständigen und unabhängigen Prüfer (TÜV SÜD Sec-IT GmbH).

Werden im Auftrag zu erhebende oder zu verarbeitende personenbezogene Daten durch Unterauftragnehmer oder Dienstleister des Auftragnehmers erhoben oder verarbeitet, ist darüber hinausgehend die Durchführung einer Dokumentenprüfung und / oder eines Audits vor Ort bei den Unterauftragnehmern oder Dienstleistern des Auftragnehmers nach Maßgabe des sachverständigen und unabhängigen Prüfers (TÜV SÜD Sec-IT GmbH) erforderlich.

Werden im Auftrag zu erhebende oder zu verarbeitende personenbezogene Daten elektronisch übermittelt oder anderweitig elektronisch bereit gestellt, kann darüber hinausgehend die Durchführung eines Schwachstellen-Scans nach Maßgabe des sachverständigen und unabhängigen Prüfers (TÜV SÜD Sec-IT GmbH) erforderlich sein.

Die Prüfungen und Bewertungen werden jährlich wiederholt.

1 vgl. § 11 Bundesdatenschutzgesetz

3 Prüfungsinhalte

Die vom Auftragnehmer im Rahmen von Auftragsdatenverarbeitungen anzuwendenden

- Leistungs- und auftragsbezogenen Dokumentationen
- Allgemeinen Maßnahmen zum Datenschutz
- Technischen und organisatorischen Maßnahmen zum Datenschutz

werden anhand unten stehender Einzelanforderungen durch einen sachverständigen und unabhängigen Prüfer (TÜV SÜD Sec-IT GmbH) geprüft und bewertet.

3.1 Leistungs- und auftragsbezogene Dokumentation

Zur geregelten und nachvollziehbaren Durchführung von Auftragsdatenverarbeitungen hat der Auftragnehmer in angemessenem und geeignetem Maße eingesetzte Infrastrukturen, Ressourcen und Prozesse schriftlich oder in elektronischer Form allgemein und sofern erforderlich auftragsbezogen zu dokumentieren. Dies beinhaltet unter anderem:

3.1.1 Der mit dem Auftraggeber geschlossene Vertrag zur Auftragsdatenverarbeitung sowie hieraus hervorgehende Einzelanweisungen des Auftraggebers hinsichtlich der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag sind dokumentiert.

3.1.2 Nachfolgende vertragliche Veränderungen hinsichtlich der Auftragsdatenverarbeitung oder nachfolgende Einzelanweisungen des Auftraggebers hinsichtlich der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag sind dokumentiert.

3.1.3 Die Art und Weise der Dienstleistungserbringung und die hieraus erfolgend notwendigen Erhebungen oder Verarbeitungen personenbezogener Daten im Auftrag sind beschrieben.

3.1.4 Die Art und Weise der Datenübermittlungen oder -Übergaben im Auftrag erhobener oder zu verarbeitender personenbezogener Daten zwischen Auftraggeber und Auftragnehmer oder mit weiteren im Rahmen der Auftragsdatenverarbeitung tätige Unterauftragnehmer oder Dienstleister des Auftragnehmers ist beschrieben.

3.1.5 Weisungsberechtigte Stellen oder Beschäftigte beim Auftraggeber und entsprechend zum Empfang von Weisungen beim Auftragnehmer berechtigte Stellen oder Beschäftigte sind benannt.

3.1.6 Die mit der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag befassten Beschäftigten des Auftragnehmers sind benannt.

3.1.7 Unterauftragnehmer oder Dienstleister des Auftragnehmers, die Zugriff auf im Auftrag erhobene oder zu verarbeitende personenbezogene Daten haben oder im Zuge von Wartungstätigkeiten beim Auftragnehmer Einsicht in diese personenbezogenen Daten nehmen könnten, sind benannt.

3.1.8 Erforderliche Handlungsschritte zur Information des Auftraggebers bei erfolgten Zuwiderhandlungen gegen Weisungen des Auftraggebers sowie bei erfolgtem Datendiebstahl, -Verlust oder -Zerstörung, insbesondere sofern hiervon § 42a Bundesdatenschutzgesetz betroffen ist, sind beschrieben.

3.2 Allgemeine Maßnahmen zum Datenschutz

Der Auftragnehmer hat allgemeine Maßnahmen zum Schutz im Auftrag zu erhebender oder zu verarbeitender personenbezogener Daten zu treffen. Diese allgemeinen Maßnahmen zum Datenschutz des Auftragnehmers orientieren sich an grundlegenden Anforderungen des Bundesdatenschutzgesetzes an Daten verarbeitende Stellen und beinhalten unter anderem:

3.2.1 Sofern gemäß § 4f Bundesdatenschutzgesetz erforderlich, ist ein Datenschutzbeauftragter schriftlich bestellt.

3.2.2 Sofern gemäß § 4d Bundesdatenschutzgesetz erforderlich, sind Vorabkontrollen der Verfahren der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag durchgeführt.

3.2.3 Datenschutz-Dokumentationen hinsichtlich der im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten sind erstellt, hierzu gehören:

- Interne Verarbeitungsübersichten zur Darstellung und Bewertung der Verfahren der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag.
- Dokumentationen von gemäß § 4d Bundesdatenschutzgesetz erforderlichen Vorabkontrollen oder anderweitigen erforderlichen internen Datenschutz-Auditierungen.
- Verfahrens- oder Arbeitsanweisungen zum Datenschutz die Auftragsdatenverarbeitung im Allgemeinen oder Einzelanweisungen des Auftraggebers die Erhebung oder Verarbeitung personenbezogener Daten im Auftrag betreffend.

3.2.4 Beschäftigte, die im Auftrag erhobene oder zu verarbeitende personenbezogene Daten erheben oder verarbeiten, sind schriftlich auf das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz verpflichtet.

3.2.5 Schulungen der Beschäftigten zum Datenschutz sind regelmäßig durchgeführt.

3.2.6 Schulungen der mit der Datenerhebung oder -Verarbeitung befassten Beschäftigten hinsichtlich der besonderen Bedingungen und Umstände der erfolgenden Auftragsdatenverarbeitungen oder Einzelanweisungen des Auftraggebers hinsichtlich der Erhebung oder Verarbeitung personenbezogener Daten im Auftrag sind durchgeführt.

3.3 Technische und organisatorische Maßnahmen zum Datenschutz

Die zu prüfenden und zu bewertenden technischen und organisatorischen Maßnahmen zum Datenschutz des Auftragnehmers orientieren sich an den Anforderungen der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz und umfassen somit technische und organisatorische Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und zur Trennungskontrolle.

3.3.1 Zutrittskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu verhindern, dass Unbefugte Zutritt erlangen können zum Betriebsgelände, zu Betriebsräumen und weiteren Infrastrukturen oder Datenverarbeitungsanlagen, -Systemen oder -Applikationen, in oder mit denen personenbezogene Daten im Auftrag erhoben oder verarbeitet werden. Dies beinhaltet unter anderem:

3.3.1.1 Zum Schutz der im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten sind geeignete bauliche und strukturelle Voraussetzungen das Betriebsgelände, die Betriebsgebäude und -Räume sowie insbesondere ausgewiesene Sicherheitsbereiche betreffend, geschaffen.

3.3.1.2 Ein Berechtigungskonzept ist erstellt, das festlegt, welche Zutrittsmöglichkeiten zum Betriebsgelände, den Betriebsräumen und insbesondere zu ausgewiesenen Sicherheitsbereichen generell vorhanden sind, welche Zutrittsberechtigungen einzelne Beschäftigte bzw. Beschäftigtengruppen oder zutrittsberechtigte Dritte innehaben und mit welchen Zutrittsmitteln die Zutritte jeweils erfolgen können.

3.3.1.3 Das Berechtigungskonzept wird an zentraler Stelle aktuell vorgehalten und ausschließlich von dieser Stelle administriert.

3.3.1.4 Der Verlust von Zutrittsmitteln ist meldepflichtig, der Verlust von Zutrittsmitteln ist dokumentiert.

3.3.1.5 Verwendete Zutrittsmittel sind kennzeichnungsfrei.

3.3.1.6 Regelungen zum Zutritt von Unterauftragnehmern, Dienstleistern oder Besuchern sind eingeführt und angewendet.

3.3.1.7 Technische Sicherungsanlagen (dies kann z. B. beinhalten: Einbruchmeldeanlagen, Alarmanlagen, Videoüberwachungsanlagen, Einbruchssicherungen) sind installiert und in Betrieb.

3.3.1.8 Außerhalb der Betriebszeiten sind geeignete technische oder organisatorische Maßnahmen zur Sicherung und Überwachung des Betriebsgeländes und der Betriebsräume etabliert.

3.3.2 Zugangskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu verhindern, dass Unbefugte Zugang erlangen können zu Datenverarbeitungsanlagen, -Systemen oder -Applikationen, mit denen personenbezogene Daten erhoben oder verarbeitet werden. Dies beinhaltet unter anderem:

3.3.2.1 Ein Konzept zur IT-Sicherheit ist erstellt (dies kann z. B. beinhalten: Definition des allgemeinen Schutzbedarfs, Darstellung der zu schützenden personenbezogenen Daten und eingesetzten Datenverarbeitungsanlagen, Dokumentation und Bewertung der bestehenden Sicherheitsmaßnahmen, Risikoanalyse, Festlegung von Verantwortlichkeiten, Befugnissen und Sicherheitszielen, Festlegung von weiterführenden Sicherheitsmaßnahmen und Wartungszyklen).

3.3.2.2 Ein Berechtigungskonzept ist erstellt, das festlegt, welche Zugangsmöglichkeiten zu den Datenverarbeitungsanlagen, -Systemen oder -Applikationen eingerichtet sind und welche Zugangsberechtigungen einzelne Beschäftigte bzw. Beschäftigtengruppen oder zugangsberechtigte Unterauftragnehmer oder Dienstleister innehaben.

3.3.2.3 Das Berechtigungskonzept wird an zentraler Stelle aktuell vorgehalten und ausschließlich von dieser Stelle administriert.

3.3.2.4 Grundsätzliche technische Sicherungsanlagen sind installiert und in Betrieb (dies kann z. B. beinhalten: Firewall, Intrusion-Detection-System, Virenschutz).

3.3.2.5 Technische Maßnahmen zur Sicherung interner Zugänge zu Datenverarbeitungsanlagen, -Systemen oder -Applikationen vor unbefugtem Zugang sind anhand des Berechtigungskonzeptes installiert und in Betrieb (dies kann z. B. beinhalten: Sicherung von USB-Schnittstellen, DVD-/CD-Laufwerken).

3.3.2.6 Technische Maßnahmen zur Sicherung externer Zugänge (z. B. WWW, VPN, FTP) zu Datenverarbeitungsanlagen, -Systemen oder -Applikationen vor unbefugtem Zugang sind anhand des Berechtigungskonzeptes installiert und in Betrieb.

3.3.3 Zugriffskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu verhindern, dass die zur Verwendung von Datenverarbeitungsanlagen, -Systemen oder -Applikationen Berechtigten Zugriff erlangen können auf personenbezogene Daten, die nicht ihren Zugriffsberechtigungen unterliegen und dass im Auftrag zu erhebende oder zu verarbeitende personenbezogene Daten durch Unbefugte eingesehen, kopiert, verändert oder gelöscht werden können. Dies beinhaltet unter anderem:

3.3.3.1 Ein Berechtigungskonzept ist erstellt, das festlegt, welche Zugriffsberechtigungen einzelne Beschäftigte bzw. Beschäftigtengruppen oder zugriffsberechtigte Dritte innerhalb der generell bestehenden Zugangsberechtigungen innehaben.

3.3.3.2 Das Berechtigungskonzept wird an zentraler Stelle aktuell vorgehalten und ausschließlich von dieser Stelle administriert.

3.3.3.3 Die Anwendung von angemessenen Authentifizierungs- und Passwortrichtlinien für den Zugriff auf Datenverarbeitungsanlagen ist anhand des Berechtigungskonzeptes festgelegt, dokumentiert und überwacht.

3.3.3.4 Richtlinien zur Arbeitsplatzsicherung sind etabliert (dies kann z. B. beinhalten: Bildschirmsperrung, Logout).

3.3.3.5 Zugriffsmittel sind sicher verwahrt bzw. gespeichert.

3.3.3.6 Die Rückgabe, Sperrung oder Löschung von im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten erfolgt nach Weisung des Auftraggebers.

3.3.3.7 Die Vernichtung von im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten erfolgt nach Weisung des Auftraggebers oder entsprechend der Schutzklassen gemäß DIN 66399.

3.3.4 Weitergabekontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu verhindern, dass im Auftrag erhobene oder zu verarbeitende personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern durch Unbefugte eingesehen, kopiert, verändert oder gelöscht werden können und die es ermöglichen festzustellen, an welche Stellen eine Übermittlung im Auftrag erhobener oder zu verarbeitender personenbezogener Daten vorgesehen ist. Dies beinhaltet unter anderem:

3.3.4.1 Die elektronische Übermittlung im Auftrag erhobener oder zu verarbeitender personenbezogener Daten ist dem aktuellen technischen Stand entsprechend verschlüsselt.

3.3.4.2 Bei Transport im Auftrag erhobener oder zu verarbeitender personenbezogener Daten mittels elektronischer oder optischer Datenträger oder mobiler Endgeräte (z. B. Festplatten, USB, DVD, CD, Notebooks) sind diese personenbezogenen Daten bzw. Datenträger verschlüsselt.

3.3.4.3 Bei Transport im Auftrag erhobener oder zu verarbeitender personenbezogener Daten mittels physischer Datenträger (Papier) sind diese personenbezogenen Daten bzw. Datenträger durch geeignete Maßnahmen geschützt.

3.3.4.4 Die Verfahren der regelmäßigen Übermittlungen im Auftrag erhobener oder zu verarbeitender personenbezogener Daten, die eingesetzten Abruf- und Übermittlungsprogramme sowie die Empfänger übermittelter personenbezogener Daten sind dokumentiert.

3.3.5 Eingabekontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass nachträglich festgestellt werden kann, ob und von wem im Auftrag erhobene oder zu verarbeitende personenbezogene Daten in Datenverarbeitungsanlagen, -Systeme oder -Applikationen eingegeben, verändert oder gelöscht worden sind. Dies beinhaltet unter anderem:

3.3.5.1 Die Datenverarbeitungsanlagen, -Systeme oder -Applikationen, mit denen im Auftrag erhobene oder zu verarbeitende personenbezogene Daten eingegeben, geändert und gelöscht werden können, sind dokumentiert.

3.3.5.2 Eingaben, Veränderungen oder Löschungen im Auftrag erhobener oder zu verarbeitender personenbezogener Daten in Datenverarbeitungsanlagen, -Systemen oder -Applikationen sind protokolliert und können anlassbezogen ausgewertet werden.

3.3.5.3 Externe Zugriffe auf Datenverarbeitungsanlagen, -Systemen oder -Applikationen mit im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten sind protokolliert und können anlassbezogen ausgewertet werden.

3.3.6 Auftragskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten, die im Auftrag erhoben oder verarbeitet werden, ausschließlich entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies beinhaltet unter anderem:

3.3.6.1 Vor Einsatz von Unterauftragnehmern oder Dienstleistern im Rahmen der Auftragsdatenverarbeitung ist geprüft, ob eine Übermittlung im Auftrag erhobener oder zu verarbeitender personenbezogener Daten an Unterauftragnehmer oder Dienstleister zulässig ist.

3.3.6.2 Sofern hinsichtlich des Einsatzes von Unterauftragnehmern oder Dienstleistern im Rahmen der Auftragsdatenverarbeitung eine Meldepflicht gegenüber dem Aufraggeber besteht, sind Unterauftragnehmer oder Dienstleister vor ihrem Einsatz an den Auftraggeber gemeldet.

3.3.6.3 Die vertragliche Einbindung von Unterauftragnehmern oder Dienstleistern im Rahmen der Auftragsdatenverarbeitung folgt den vertraglichen Vorgaben des Aufragnehmers hinsichtlich der Auftragsdatenverarbeitung.

3.3.6.4 Die Prüfung und Bewertung getroffener technischer und organisatorischer Maßnahmen zum Datenschutz bei Unterauftragnehmern oder Dienstleistern folgt den vertraglichen Vorgaben des Aufragnehmers hinsichtlich der Auftragsdatenverarbeitung.

3.3.6.5 Bei erfolgten Zuwiderhandlungen gegen Weisungen des Auftraggebers sowie bei erfolgtem Datendiebstahl, -Verlust oder -Zerstörung, insbesondere sofern hiervon § 42a Bundesdatenschutzgesetz betroffen ist, erfolgt eine Information des Auftraggebers.

3.3.7 Verfügbarkeitskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu verhindern, dass im Auftrag erhobene oder zu verarbeitende personenbezogene Daten zufällig zerstört werden oder verloren gehen. Dies beinhaltet unter anderem:

3.3.7.1 Ein Konzept für den Umgang mit Betriebsstörungen und Notfällen ist erstellt (dies kann z. B. beinhalten: Notfallplan für Notfallszenarien, Festlegung von Verantwortlichkeiten und Befugnissen für beschriebene Notfälle, Beschreibung von Maßnahmen zur Notfallerkennung und von Benachrichtigungswegen).

3.3.7.2 Es sind wirksame und angemessene Maßnahmen zur allgemeinen Datensicherung eingeführt und umgesetzt (dies kann z. B. beinhalten: Planung und Durchführung von erforderlichen Wartungen, unterbrechungsfreie Stromversorgung, Klimatisierung, Feuerschutz, Brandmeldeeinrichtungen, Löscheinrichtungen, Wassereinbruchsschutz).

3.3.7.3 Es sind wirksame und angemessene Maßnahmen zur erweiterten Datensicherung eingeführt und umgesetzt (dies kann z. B. beinhalten: Aufbau von Redundanzen, Backup).

3.3.7.4 Die Wiederherstellung von gespeicherten im Auftrag erhobenen oder zu verarbeitenden personenbezogenen Daten ist regelmäßig geprüft, die Ergebnisse der Prüfung sind dokumentiert.

3.3.7.5 Schadens- und Störfälle von Datenverarbeitungsanlagen, -Systemen oder -Applikationen sind dokumentiert.

3.3.8 Trennungskontrolle

Auftragnehmer von Auftragsdatenverarbeitungen haben technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass zu verschiedenen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies beinhaltet unter anderem:

3.3.8.1 Das Betriebsgelände, die Betriebsgebäude und -Räume erlauben eine räumliche Trennung nach unterschiedlichen Funktionsbereichen und Sicherheitsbereichen entsprechend der Verarbeitungen im Auftrag erhobener oder zu verarbeitender personenbezogener Daten.

3.3.8.2 Die organisatorische und technische Trennung der Erhebung und Verarbeitung im Auftrag erhobener oder zu verarbeitender personenbezogener Daten nach Mandanten ist gewährleistet.

3.3.8.3 Die Trennung von Produktiv-, Entwicklungs- und Testsystemen ist gewährleistet. Im Auftrag erhobene oder zu verarbeitende personenbezogene Daten sind nicht zu Entwicklungs- oder Testzwecken verwendet.

3.3.8.4 Bei pseudonymisierten im Auftrag erhobenen oder zu verarbeitenden personenbezogener Daten erfolgt die Aufbewahrung der Zuordnungsinformationen von diesen getrennt.

4 Geltungsbereich, Zertifikatsvergabe, Gültigkeit der Zertifikate

Zertifizierbar sind ausschließlich Erhebungen oder Verarbeitungen personenbezogener Daten, die vollumfänglich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgen.

Der Geltungsbereich der Prüfung, Bewertung und Zertifizierung insgesamt ist beschränkt auf das beim Auftragnehmer jeweils geprüfte und bewertete Verfahren der Auftragsdatenverarbeitung und die in diesem Zusammenhang seitens des Auftragnehmers erstellten leistungs- und auftragsbezogenen Dokumentationen sowie die getroffenen allgemeinen, technischen und organisatorischen Maßnahmen zum Datenschutz und ist auf den jeweiligen Zertifikaten dargestellt.

Das Zertifikat „Zertifizierte Auftragsdatenverarbeitung“ erhalten Auftragnehmer von Auftragsdatenverarbeitungen erst nach einer sorgfältigen und erfolgreich abgeschlossenen Prüfung und Bewertung der im Rahmen von Auftragsdatenverarbeitungen erstellten leistungs- und auftragsbezogenen Dokumentationen sowie der getroffenen allgemeinen, technischen und organisatorischen Maßnahmen zum Datenschutz gegen oben dargestellte Anforderungen durch einen sachverständigen und unabhängigen Prüfer (TÜV SÜD Sec-IT GmbH) und Freigabe durch die Fachzertifizierungsstelle der TÜV SÜD Sec-IT GmbH.

Das Zertifikat wird durch die Fachzertifizierungsstelle der TÜV SÜD Sec-IT GmbH erteilt. Die Gültigkeit der Zertifikate ist auf ein Jahr beschränkt, sofern auf den jeweiligen Zertifikaten nichts anderes vermerkt ist.

5 Ausschlüsse, abschließende Bemerkungen

Die oben dargestellten Anforderungen haben sich im Wesentlichen an den gesetzlichen Regelungen und Vorgaben zum Datenschutz zu orientieren. Aus diesem Grunde enthält der Anforderungskatalog auch dem Gesetzeswortlaut entsprechende Formulierungen und Anforderungen. Die oben dargestellten Anforderungen übersteigen jedoch die Anforderungen von § 11 Bundesdatenschutzgesetz und der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz an Auftragnehmer von Auftragsdatenverarbeitungen.

Das Zertifikat „Zertifizierte Auftragsdatenverarbeitung“ erhalten Auftragnehmer von Auftragsdatenverarbeitungen erst nach einer sorgfältigen und erfolgreich abgeschlossenen Prüfung und Bewertung durch einen sachverständigen und unabhängigen Prüfer (TÜV SÜD Sec-IT GmbH). Dennoch kann TÜV SÜD Sec-IT GmbH keine Garantie übernehmen, dass alle dieser Zertifizierung zugrundeliegenden oben dargestellten Anforderungen von den geprüften und zertifizierten Auftragnehmern durchgängig eingehalten werden.

Die Vergabe des Zertifikats „Zertifizierte Auftragsdatenverarbeitung“ der TÜV SÜD Sec-IT GmbH an Auftragnehmer von Auftragsdatenverarbeitungen ersetzt nicht eine schriftliche Auftragserteilung an die Auftragnehmer gemäß § 11 Bundesdatenschutzgesetz durch die jeweiligen Auftraggeber. Die Vergabe des Zertifikats „Zertifizierte Auftragsdatenverarbeitung“ der TÜV SÜD Sec-IT GmbH an Auftragnehmer von Auftragsdatenverarbeitungen ersetzt ggf. nicht eine abschließende Beurteilung der Angemessenheit der seitens der Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz durch die jeweiligen Auftraggeber der Auftragsdatenverarbeitungen, da entsprechende Maßnahmen ggf. im Kontext der konkreten Beauftragungsfälle im Einzelnen zu bewerten und vom jeweiligen Schutzbedarf der im Auftrag erhobenen oder verarbeiteten personenbezogenen Daten abhängig sind.

Die Vergabe des Zertifikats „Zertifizierte Auftragsdatenverarbeitung“ ersetzt nicht eine rechtliche, steuerrechtliche oder betriebswirtschaftliche Beratung. TÜV SÜD Sec-IT GmbH weist ferner ausdrücklich darauf hin, dass mit dem Auftrag zur Prüfung und Bewertung der eingesetzten Verfahren ein Auftrag im Sinne einer rechtlichen Beratung nicht einhergeht; individualisierte rechtliche Empfehlungen oder rechtliche Hinweise werden nicht gegeben. Die Prüfung und Bewertung der eingesetzten Verfahren der Auftragnehmer beinhaltet keine rechtliche Prüfung im Sinne des Rechtsberatungsgesetzes, insbesondere findet keine Prüfung und Bewertung der eingesetzten Verfahren auf deren datenschutzrechtliche Zulässigkeit statt.