Allgemeine Vorschriften Datenschutz und Datensicherheit (AVDD)

(Stand: Juni 2015)

1 Präambel
Der Gesetzgeber hat § 11 BDSG (Bundesdatenschutzgesetz) novelliert. Diese Änderungen stellen an den Kunden (nachfolgend: Auftraggeber) zusätzliche Anforderungen. Der Auftraggeber hat bei Missachtung mit empfindlichen Bußgeldern bis hin zum Verbot der Datenverarbeitung zu rechnen. Obschon es sich bei Wartung, Pflege und Service nicht um eine Auftragsdatenverarbeitung im engeren Sinne handelt, müssen wegen § 11 Abs. 5 BDSG die strengen Regeln der Auftragsdatenverarbeitung dennoch eingehalten werden. Die GSD Gesellschaft für Software, Entwicklung und Datentechnik mbH (nachfolgend: Auftragnehmer) unterstützt den Auftraggeber bei der Einhaltung dieser gesetzlichen Anforderungen, indem sie es dem Auftraggeber mit den diesseitigen Allgemeinen Vorschriften Datenschutz und Datensicherheit ermöglicht, die gesetzlichen Anforderungen des § 11 BDSG umzusetzen.

2 Vertragliche Beziehungen
Zwischen dem Auftraggeber und Auftragnehmer werden als Ergänzung zu allen zwischen den Parteien bestehenden Vereinbarungen, anlässlich derer der Auftragnehmer oder durch ihn beauftragte Dritte in Kontakt mit personenbezogenen Daten im Sinne des Bundesdatenschutzgesetzes kommt, die nachfolgenden Regelungen getroffen. Betroffene Verträge sind insbesondere Fernwartungsvereinbarungen.

3 Definitionen
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
Datenverarbeitung im Auftrag ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.
Erheben ist das Beschaffen von Daten über den Betroffenen.
Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.
Löschen ist das Unkenntlich machen gespeicherter personenbezogener Daten.
Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

4 Gegenstand, Dauer des Auftrages, Umfang, Art und Zweck, etc.

4.1 Gegenstand
Gegenstand der Verträge gem. Ziff. 2 ist es, Wartungsarbeiten im Wege des Fernzugriffs beim oder für den Auftraggeber am im Einsatz befindlichen EDV-System zu ermöglichen.

4.2 Dauer
Die Dauer der einzelnen Verträge ergibt sich aus den jeweiligen Vereinbarungen.

4.3 Umfang, Art, Zweck der Erhebung
Anlässlich der Durchführung der betroffenen Verträge ist es nicht ausgeschlossen, dass der Auftragnehmer rein zufällig Kenntnis von personenbezogenen Daten erhält. Im Übrigen erhebt oder verarbeitet der Auftragnehmer keine personenbezogenen Daten des Auftraggebers.

4.4 Arten der Daten und Kreis der Betroffenen
Die durch den Auftraggeber erzeugten Daten können sowohl „einfache“ personenbezogene Daten darstellen als auch besondere personenbezogene Daten (sensible Daten) im Sinne von § 3 Abs. 9 BDSG sein. Der Kreis der Betroffenen kann insbesondere Beschäftigte, Kunden, Lieferanten und Interessenten der Auftraggeberin umfassen.

4.5 Berichtigung, Sperrung und Löschung von Daten
Der Auftragnehmer wird ohne Weisung des Auftraggebers keine Berichtigung, Sperrung oder Löschung von Daten vornehmen. Die Parteien stellen klar, dass eine solche Nutzung nicht Gegenstand der Verträge i. S. v Ziffer 2 ist.

5 Weisungen des Auftraggebers
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Der Auftraggeber ist berechtigt, vollumfänglich Weisungen zu erteilen. Mündliche Weisungen hat der Auftraggeber schriftlich zu bestätigen.

6 Datengeheimnis
Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers den Datenschutz gemäß Bundesdatenschutzgesetz (BDSG) sowie gem. § 91 ff. Telekommunikationsgesetz (TKG) sowie ggf. Sondergesetzen wie z.B. SGB V, zu wahren. Er verpflichtet sich also, die gleichen Geheimschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Soweit der Auftraggeber Sondergesetzen des Datenschutzes unterliegt, die über Bundesdatenschutzgesetz, Telemediengesetz (TMG) und Telekommunikationsgesetz hinausgehen, ist der Auftraggeber verpflichtet, den Auftragnehmer auf die Geltung dieser Gesetze ausdrücklich hinzuweisen. Der Auftragnehmer wird sodann unverzüglich seine daraus folgenden Verpflichtungen feststellen und einhalten. Er wird nur Mitarbeiter beschäftigen, deren Zuverlässigkeit und Vertrauenswürdigkeit er sich zuvor versichert hat. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die Einhaltung der datenschutzrechtlichen Vorschriften überwacht. **Der Auftragnehmer sichert zu, dass seine mit der Verarbeitung der Daten des Auftraggebers beschäftigten Mitarbeiter stets gemäß § 5 BDSG sowie gem. § 88 TKG schriftlich auf das Daten und Fernmeldegeheimnis verpflichtet sind.**
Die Verarbeitung von Daten für den Auftraggeber ist nur in den dafür vorgesehenen Betriebsräumen des Auftragnehmers zulässig.
Die Verarbeitung und Nutzung der Daten finden ausschließlich im Gebiet der Bundesrepublik Deutschland oder in Ländern mit angemessenem Datenschutzniveau statt. Aktuell gilt dies für Mitgliedsstaaten der Europäischen Union bzw. den Staaten des Europäischen Wirtschaftsraums. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.
Auskünfte über Daten und Gegebenheiten im Zusammenhang mit der Auftragsausführung des Auftragnehmers für den Auftraggeber darf der Auftragnehmer Dritten gegenüber nur nach vorheriger schriftlicher Zustimmung erteilen. In diesem Vertrag ausdrücklich geregelte oder gesetzlich vorgeschriebene Auskunftsrechte bzw. Auskunftspflichten bleiben hiervon unberührt. Auskünfte nach Datenschutzrecht erteilt allein die Auftraggeberin als verantwortliche Stelle. An der Erstellung notwendiger Verfahrensverzeichnisse bzw. Verarbeitungsbeschreibungen hat der Auftragnehmer auf Anforderung des Auftraggebers mitzuwirken. Er hat dem Auftraggeber insoweit die erforderlichen Angaben zuzuleiten. Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der in diesem Vertrag vereinbarten sowie der allgemeinen technischen und organisatorischen Maßnahmen nach § 9 BDSG zu. Er wird also seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen. Der Auftragnehmer dokumentiert von Ihm ergriffene Maßnahmen zur Einhaltung seiner Verpflichtungen aus den vorstehenden Ziffern schriftlich und nachvollziehbar.

7 Geschäftsgeheimnis

Der Auftragnehmer verpflichtet sich, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des Auftraggebers (Geschäftsgeheimnisse) Verschwiegenheit zu wahren. Er wird auch seine Mitarbeiter zur Verschwiegenheit verpflichten. Dem Auftraggeber bleibt es unabhängig davon unbenommen, entsprechende Verschwiegenheitsverpflichtungen direkt mit den Mitarbeitern des Auftragnehmers zu vereinbaren.

8 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Maßnahmen (TOM) zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den Forderungen der Anlage zu § 9 Satz 1 BDSG entsprechen (Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits-kontrolle und Trennungsgebot). Eine Maßnahme der Zugangs-, Zugriffs- und Weitergabekontrolle ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Insbesondere sichert der Auftragnehmer die Einhaltung der TOM zu, die er in der Anlage **Selbstauskunft TOM** aufgeführt hat. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insbesondere ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

8.1 Nutzung von Zertifikaten (z.B. ISO 27001, ISA+), Testaten und Selbstauskünften

Verfügt der Auftragnehmer über ein datenschutzrelevantes Zertifikat, kann dieses unter folgenden Voraussetzungen zur Unterstützung der Vorabkontrollen und Überwachungen durch den Auftraggeber genutzt werden:

1. Das Zertifikat muss gültig sein.
2. Die Auftragsdatenverarbeitung des Auftragsnehmers muss im Scope der Zertifizierung liegen.
3. Das Statement of Applicability (SoA) darf keine Ausschlüsse betreffend der in der Anlage zu §9 Satz 1 BDSG genannten TOM aufweisen.

Ebenso können Datenschutz-Testate von sachverständigen Dritten sowie Selbstauskünfte des Auftragnehmers Verwendung finden.

Bitte beachten Sie, dass Zertifikate, Testate und Selbstauskünfte die Vorabkontrolle und Überwachung durch den Auftraggeber erheblich erleichtern, jedoch nicht ersetzen.

9 Ansprechpartner

Die Parteien sind sich darüber einig, dass es notwendig ist, Regelungen zur Kommunikation zu treffen, um eine sichere, störungsfreie und datenschutzgerechte Auftragsausführung zu gewährleisten. Der Auftragnehmer hat den Auftraggeber vor wichtigen Eingriffen in das System vom Auftraggeber über beabsichtigte Änderungen und Eingriffe unverzüglich zu informieren und diese nach entsprechender Freigabe durch den Auftraggeber zu veranlassen bzw. durchzuführen. Die Parteien benennen wechselseitig Ansprechpartner und werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen. Der Auftragnehmer darf Auskünfte ausschließlich gegenüber den vom Auftraggeber autorisierten Personen erteilen. Der Auftragnehmer verpflichtet sich durch organisatorische wie technische Maßnahmen sicherzustellen, dass nur die benannten Mitarbeiter Zugang zu den zu betreuenden Systemen des Auftraggebers erlangen können.

10 Pflichten, Kontroll- und Betretungsrechte

Der Auftragnehmer arbeitet datenschutzrechtlich ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Er verwendet etwaige zur Verarbeitung überlassene Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und sonstige Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Durchführung des Auftrages erforderlich sind, sowie Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften, Testat eines Sachverständigen und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten datenschutzrechtlich relevante Unterlagen und erstellten datenschutzrechtlich relevante Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis im Sinne von Ziffer 2 stehen, dem Auftraggeber auszuhändigen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung beziehungsweise Übergabe. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe, Löschung oder Aufbewahrung der Daten, so trägt diese der Auftraggeber.

11 Subunternehmer/Unterauftragnehmer

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag an diese zu übertragen. Erst danach ist eine Weiterleitung von Daten zulässig.

Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Dem Auftraggeber werden Kontroll- und Überprüfungsrechte entsprechend Ziffer 10 eingeräumt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer von Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen u.a. Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene schriftliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

12 Informationspflichten, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als verantwortlicher Stelle im Sinne des Bundesdatenschutzgesetzes liegen. Es gilt deutsches Recht.

Technische und organisatorische Maßnahmen (TOM)
Thema Datenschutz und Datensicherheit nach § 9 BDSG

Stand: Mai 2015

1 Zutrittskontrolle

Maßnahmen:

- Zutritt zu Datenverarbeitungsanlagen durch Türsicherung
- Schlüsselvergabe an berechtigte Mitarbeiter wird protokolliert
- Gebäude Zu- und Ausgänge durch Videoüberwachung (außerhalb der Betriebszeiten)
- Fremdpersonal, u.a. Lieferanten und IT-Service wird durch GSD Mitarbeiter beaufsichtigt

2 Zugangskontrolle

Maßnahmen:

- Userkennung durch sicheres Passwort (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts gemäß Arbeitsrichtlinie)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Firewall
- Protokollierung von Benutzern und Rechten (Sicherheitsrichtlinie über Domäne)
- Regelung zur E-Mail- und Internetnutzung gemäß Arbeitsrichtlinie

3 Zugriffskontrollen

Maßnahmen:

- Berechtigungsprofil, nach DOCUframe-Gruppen differenziert nach Lese- und Schreibberechtigung dokumentiert sowie Vertretungsregelung (Group-Policies + DOCUframe Gruppenzugehörigkeit)

4 Weitergabekontrolle

Maßnahmen:

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Bei Datenträgertransporte, Verschlüsselung der Daten durch Passwort
- Übergabeprotokoll bzw. Ein-Ausgangsprotokoll für Datenträger
- Schutz der Schnittstellen von PCs, USB-Sticks gemäß Arbeitsrichtlinie
- Löschung, Vernichtung von Datenträger gem. Arbeitsrichtlinie
- Bei Fernwartung entsprechend den Kundenvorgaben und Home-Office-Betrieb wird der Zugriff auf Kundendaten via VPN gesichert

5 Eingabekontrolle

Maßnahmen:

- Windows-Protokoll der Einwahlvorgänge in Kundensysteme
- Die Eingabe der Daten wird datenfeldbezogen, datensatzbezogen und dateibezogen protokolliert

6 Auftragskontrolle

Maßnahmen:

- Eindeutige Vertragsgestaltung zur Durchführung des Kundenauftrages
- Formalisierte Auftragserteilung (Auftragsformular und via Internetportal)
- Kontrolle der Auftragsausführung mit GSD Projektmanagement-Tool

7 Verfügbarkeitskontrolle

Maßnahmen:

- Backup-Verfahren gemäß GSD Sicherheitsrichtlinie
- Spiegeln von Festplatten, z.B. RAID-Verfahren, regelmäßige Sicherungskopien, getrennte Aufbewahrung (Tresor für Datenträger und ausgelagerte Festplatten nach Brandprüfung gemäß ECB:S/EN) sowie extern in Banktresor
- Virenschutz / Firewall
- Notfallplan mit Alarmierungs- und Wiederanlaufregelung gemäß GSD Sicherheitsrichtlinie
- Sicherung des Serverraumes durch unterbrechungsfreie Stromversorgung (USV)
- Brandschutz Feuerlöscheinrichtungen und automatisches Herunterfahren der Systeme

8 Trennungskontrolle

Maßnahmen:

- "Interne Mandantenfähigkeit" auf Anwendungsebene
- Funktionstrennung zwischen Produktions- & Testsystem