

Teil I – Allgemeine Regelungen

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz und zur Datensicherheit, die sich aus der im Dienstvertrag/Mietvertrag/Werkvertrag (Hauptvertrag) in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages.

Die technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen im Sinne von Teil II dieser Vereinbarung werden permanent fortgeschrieben und ggf. neuen Entwicklungen sowohl in rechtlicher als auch in technischer Hinsicht angepasst.

§ 1 Definitionen

1. Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

2. Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

3. Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

2. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber während der Laufzeit des Vertrages und mit Beendigung des Vertrages die

Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

3. Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten nur im Rahmen des Auftrags und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke.

2. Der Auftragnehmer ist verpflichtet, den Weisungen aus dem Vertrag und den im Einzelfall erteilten Weisungen des Vertragspartners im Sinne Teil I § 1 dieses Dokuments zu folgen. Weisungen dürfen nur durch die Geschäftsführung (nachfolgend „**Weisungsberechtigte**“ genannt) erteilt werden. Die Weisungsberechtigten haben jederzeit das Recht, in Schriftform gegenüber dem Auftragnehmer weitere Weisungsberechtigte zu bestimmen. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen gesetzliche Vorschriften und/oder den Hauptvertrag verstößt, so ist der Auftragnehmer verpflichtet, den Auftraggeber hierauf unverzüglich hinzuweisen, sowie berechtigt, die Ausführung der Weisung bis zu einer schriftlichen Bestätigung der Weisung durch einen Weisungsberechtigten des Auftraggebers auszusetzen.

3. 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 zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, 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 (Zugriffskontrolle),

d) dafür Sorge zu tragen, 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 Übermitt-

lung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindungskontrolle).

Eine Maßnahme nach b) bis d) ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen ist in Teil II – Datenschutz- und Datensicherungsmaßnahmen dieser Anlage enthalten.

4. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung.

5. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

6. Der Auftragnehmer teilt dem Auftraggeber auf Anfrage die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit. Die Kontaktdaten werden zudem im Internetauftritt des Auftragnehmers veröffentlicht.

7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Datenschutzverletzungen sowie bei Verdacht auf erhebliche Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers, sofern und soweit dessen Daten davon betroffen sind.

8. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie unbefugten Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte bezüglich überlassener Datenträger zu erteilen.

9. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

10. Die Speicherung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. 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.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber und der Auftragnehmer sind bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

3. Die Pflicht zur Führung des öffentlichen Verzeichnisses gemäß § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

4. Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.

5. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrags vertraglich oder durch Weisung fest.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt:

1. der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und

2. der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

§ 6 Kontrollen

1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Hierfür kann er

a) Selbstauskünfte des Auftragnehmers einholen oder

b) sich vom Auftragnehmer ein vorhandenes Testat eines Sachverständigen, einer Wirtschaftsprüfungsgesellschaft oder einer sonstigen hierfür befugten Stelle vorlegen lassen, oder

c) nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten in den Betriebsstätten des Auftragnehmers ohne Störung des Be-

triebsablaufes eine Prüfung durchführen.

2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

3. Der Auftragnehmer ist berechtigt, den dabei entstehenden Aufwand entsprechend der zu diesem Zeitpunkt aktuellen Aareon-Preisliste in Rechnung zu stellen. Der Auftraggeber ist verpflichtet, die Auskünfte vertraulich zu behandeln. Der Auftragnehmer ist berechtigt, die Bereitstellung der Auskünfte von dem vorherigen Abschluss einer vertragsstrafenbewehrten Geheimhaltungsvereinbarung abhängig zu machen.

§ 7 Subunternehmer

1. Die Einschaltung von Subunternehmern ist aufgrund vielfältiger und hoch spezialisierter Aufgabenstellungen im IT-Bereich notwendig. Die Einschaltung von Subunternehmern (Unterauftragnehmer) durch den Auftragnehmer ist daher erlaubt.

2. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. verbundene Unternehmen mit Leistungen unterbeauftragt.

3. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Der Auftragnehmer teilt dem Auftraggeber auf Anfrage die Namen der Subunternehmer mit, die im Rahmen der hier geregelten Auftragsdatenverarbeitung mit der Erbringung von wesentlichen Leistungen beauftragt wurden.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. 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.

2. Sollten Bestimmungen dieser Vereinbarung unwirksam sein oder werden, oder sollten sich in der Vereinbarung Lücken herausstellen, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung eventueller Lücken soll eine angemessene Regelung gelten, die, soweit rechtlich möglich, dem am Nächsten kommt, was die Beteiligten

nach dem Sinne dieser Vereinbarung gewollt haben.

3. Änderungen und Ergänzungen dieser Anlage und all ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf diese Formerfordernisse.

4. Es gilt deutsches Recht.

Teil II – Technische und organisatorische Maßnahmen zur Gewährleistung von Datenschutz- und Datensicherheit (gem. § 9 BDSG)

§ 9 Organisatorische Maßnahmen

1. Der Auftragnehmer trifft sowohl in baulicher, personeller, organisatorischer als auch technischer Hinsicht erforderliche Vorkehrungen, um die Einhaltung der Datensicherheit und des Datenschutzes der im Auftrag verarbeiteten Daten sowie einen ungestörten Betriebsablauf zu gewährleisten.

2. Zur organisatorischen Sicherstellung angemessener Qualitätsstandards im Rechenzentrumsbetrieb betreibt der Auftragnehmer ein internes Kontrollsystem.

3. Es sind betriebliche Datenschutzbeauftragte (§ 4f BDSG) bestellt, die die Einhaltung der gesetzlichen Datenschutzvorschriften überwachen. Zu deren Aufgabenbereich gehören die Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen, die Führung des Verzeichnisses, die Vorabkontrolle bei besonderen Verarbeitungen sowie das Vertrautmachen der Mitarbeiter mit den Anforderungen des Datenschutzes. Weitere interne Datensicherheits- und Kontrollorgane (IT-Sicherheitsbeauftragter, Revision) werden unterstützend tätig.

4. Alle Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis (§ 5 BDSG) verpflichtet.

§ 10 Auftragskontrolle

1. Innerhalb der Systeme ist technisch sichergestellt, dass die zu verarbeitenden Daten entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben werden. Ausnahmen vom konkreten Weisungsrahmen gelten für technisch notwendige Verarbeitungen wie beispielsweise für die interne Datensicherung. Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, müssen gesondert schriftlich vereinbart werden.

2. Kompetenzen und Pflichten von Auftragnehmer und Auftraggeber sind durch einen Vertrag abgegrenzt. Der Auftragnehmer verpflichtet sich, die gespeicherten und verarbeiteten Daten zu keinen anderen Zwecken als zur Erfüllung dieses Vertrages zu verwenden.

3. Bei der Datenverarbeitung mithilfe von Endgeräten, die beim Auftraggeber aufgestellt sind, erfolgt die Eingabe und die Auswahl der Verarbeitungsvorgänge durch Mitarbeiter des Auftraggebers. Bei Aufträgen des Auftraggebers wird geprüft, dass dazu gegenüber dem Auftragnehmer bevollmächtigte Mitarbeiter des Auftraggebers die Freigabe der Aufträge erteilt haben.

§ 11 Zutrittskontrolle

1. Die Betriebsareale des Auftragnehmers sind in mehrere Sicherheitsbereiche mit differenzierten Zutrittsberechtigungen aufgeteilt.

2. Die Zutrittsberechtigungen werden nach einem Zutrittsberechtigungskonzept gesteuert. Der Zutritt zu den baulich abgeschotteten und elektronisch überwachten Sicherheitszonen des Rechenzentrums ist nur den Personen möglich, die hier notwendige Tätigkeiten ausüben.

3. Der Zutritt zu den Betriebsstätten des Auftragnehmers wird über ein Zutrittskontrollsystem geregelt (Berechtigungskarten für den Zutritt zu den Betriebsstätten und je nach Berechtigung zu verschiedenen Sicherheitsbereichen). Jede Benutzung einer Kartenabfragestation wird protokolliert.

4. Außerhalb der Regelarbeitszeit überwachen mit Bewegungsmeldern gekoppelte Videokameras Zutrittswege zu schutzbedürftigen Gebäudeteilen.

§ 12 Zugangskontrolle

1. Der Zugang zu den Anwendungssystemen ist nur nach Authentifizierung über einen Benutzer-Account mit Passwort möglich, das nach einem festgelegten Intervall vom Anwender geändert werden muss. Der Zugang ist benutzerspezifisch auf jeweils freigeschaltete Instanzen (Mandanten) beschränkt.

2. Anmeldevorgänge werden protokolliert.

§ 13 Zugriffskontrolle

1. Die Anwendungen sind so eingerichtet, dass sie ausschließlich von berechtigten Benutzern nach Eingabe eines Passworts aufgerufen werden können.

2. Die Zugriffsberechtigungen innerhalb der Anwendungen werden durch differenzierte, fachspezifische Berechtigungssysteme verwaltet.

3. Die Gestaltung von anwenderbezogenen Funktionsberechtigungen sowie die Vergabe und Anpassung von Benutzeraccounts liegen in der Verantwortung des Auftraggebers.

4. Der Kreis der privilegierten Support-Benutzeraccounts wird restriktiv auf das notwendige Maß beschränkt und unterliegt zusätzlichen Protokollmechanismen.

5. Die Serversysteme des Auftragnehmers sind durch ein mehrstufiges Firewallsystem vor unberechtigten Zugriffen aus dem Internet geschützt. Der Zugriff auf Anwendungsprogramme über das Internet wird vom Firewallsystem kontrolliert und ist durch zusätzliche Authentifizierungsmechanismen abgesichert. Der Zugriff auf Anwendungen über das Internet erfolgt verschlüsselt.

§ 14 Eingabekontrolle

Datenänderungen werden inklusive Erfassungszeitpunkt protokolliert.

§ 15 Weitergabekontrolle

1. Datenträger und Verarbeitungsergebnisse werden in geeigneten Behältnissen versandt.

2. Leitungen, Anschlüsse und Verteiler für Datenfernübertragung in den Betriebsstätten des Auftragnehmers liegen in nicht frei zugänglichen Sicherheitsbereichen.

3. Datenübertragungen laufen über Leitungen eines Netzbetreibers oder über öffentliche Netze. Durch Filtermaßnahmen und Authentifizierungsmechanismen auf den Netzwerkkomponenten sind die vom Auftragnehmer betriebenen Systeme vor dem Aufbau unberechtigter Datenfernübertragungsverbindungen geschützt.

4. Entsorgungsgut mit schutzwürdigem Inhalt wird in verschlossenen Spezialbehältern, die von außen nicht zugänglich sind, turnusmäßig von einem Unternehmen, das für diesbezügliche Tätigkeiten zertifiziert ist und den gesetzlichen Datenschutzbestimmungen unterliegt, der Vernichtung zugeführt.

5. Datenträger (Bandkassetten, optische Medien etc.) werden in besonderen Sicherheitsbereichen aufbewahrt.

6. Übermittlungen personenbezogener Daten an staatliche Einrichtungen und Behörden erfolgen nur im Rahmen entsprechender Rechtsvorschriften und werden i. d. R. durch den Auftraggeber initiiert.

§ 16 Verfügbarkeitskontrolle

1. Es sind angemessene Brandschutz-, Verlustsicherungs- und Katastrophenschutzmaßnahmen umgesetzt. Hierzu gehören unter anderem die Absicherung von RZ-Räumen durch Brandfrüherkennung, aktive Brandverhinderung bzw. Löschsysteme sowie eine autarke Notstromversorgung zur unterbrechungsfreien Überbrückung von Stromausfällen.

2. Die Anwendungsdaten werden mindestens werktäglich gesichert und in geeigneten Datensicherungsräumen gelagert.

3. Eingehende Datenträger werden auf Viren geprüft. Eingehende E-Mails und Attachments werden vor der Überführung in das allgemeine Netz für die Bürokommunikation (LAN) auf Viren geprüft. Zusätzlich sind Virenprüfprogramme sowohl an den Arbeitsstationen der Mitarbeiter als auch auf den zentralen Servern im Einsatz.

§ 17 Zweckbindungskontrolle

1. In den Anwendungssystemen der Auftragsdatenverarbeitung erfolgt eine strikte Mandantentrennung.

2. Durch das bestehende Berechtigungskonzept und die vorhandenen Benutzerberechtigungen ist eine logische Trennung von Daten, die zu unterschiedlichen Zwecken erhoben und getrennt verarbeitet werden, möglich.

3. Das Prinzip der Funktionstrennung ist angemessen innerhalb der Organisationseinheiten verwirklicht. Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist. Zur Sicherstellung werden Rechteprofile für die verschiedenen Funktionsbereiche zugeteilt und zentral administriert.