**Anlage 3 zum EVB-IT Systemlieferungsvertrag**

# RICHTLINIE INFORMATIONSSICHERHEIT

## bei der Erbringung von Systemserviceleistungen

Vergabenummer: 2025-116

Version / Datum: 1.3.0 – 6.02.2026

Präambel

Bei der Ausführung von Systemserviceleistungen oder dem Kauf von Cloud- der Software as a Service (SaaS) -Diensten kann nicht ausgeschlossen werden, dass personenbezogene Daten durch den Auftragnehmer (AN) oder seinen Unterauftragnehmern zur Kenntnis genommen werden können. Dies kann z. B. bei der Ausführung von Datensicherungs- und Migrationsmaßnahmen oder der Etablierung von Softwareschnittstellen zu unternehmensweiten Anwendungen (ERP-Systemen, Verzeichnisdiensten etc.) der Fall sein. Auch bei der Verwendung von moderner Betriebsmanagementanwendungen und IT-Sicherheitsanwendungen müssen zur Feststellung von Fehlerursachen Daten korreliert betrachtet werden, die u. U. auch eine Auflösung pseudonymisierter Identitäten erfordert.

In der Praxis kann daher bei der Ausführung der Tätigkeiten der ANs keine Unterscheidung zwischen einer Auftragsverarbeitung und einer „beiläufigen“ Kenntnisnahme“ unterschieden werden.

Die Vertragsparteien vereinbaren daher, dass die Informationssicherheit auf Basis der nachfolgenden Regelungen mit einem angemessenen Mindestgrundschutz sichergestellt und die ordnungsgemäße Ausführung nach objektiven Kriterien durch zuständige Stellen bedarfsgerecht validiert werden kann.

Diese Anlage zum EVB-IT Systemlieferungsvertrag (Hauptvertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag und den konkreten Abrufaufträgen ergeben können.

# 1 Allgemeines

## 1.1 Bezug zum Hauptvertrag

Bei der Ausführung der Leistungen gelten grundsätzlich die Bedingungen des EVB-IT Systemlieferungsvertrages. Gemäß Nr.12.2 (Allgemeine Sicherheitsanforderungen) und Nr.18.6 (Datenschutz...) des EVB-IT Systemlieferungsvertrag sind ergänzend notwendige Ausführungs-bestimmungen gesondert zu vereinbaren. Sofern nicht anders in den Abrufen vereinbart, sind bei der Ausführung der Leistungen die folgenden Aspekte durch den AN zu berücksichtigen.

## 1.2 Rechtliche Einordnung

Durch den AN ist die Einhaltung der folgenden Gesetze

- Europäische Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz (LDSG)

und dieser Richtlinie sicherzustellen, sofern die dort definierten Aufgaben, Tätigkeiten und Verantwortlichkeiten in seinen Sphärenbereich anzusiedeln sind und die Leistungserbringung Bestandteil einer Abrufauftrages sind.

## 1.3 Begriffsdefinition

Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

Der Begriff „Verwendung“ und „Verarbeitung“ umfasst auch die mögliche Kenntnisnahme, Sicherung und Wiederherstellung dieser Daten, die bei der Erbringung von Systemserviceleistungen oder SaaS-/Clouddiensten durch den AN oder von ihm beauftragten Dritten ausgeführt werden.

Der Begriffe „Auftragsdatenverarbeitung“, Auftragsverarbeitung“ oder „Verarbeitung im Auftrag“ sind inhaltlich gleichgestellt.

# 2 Gegenstand des Auftrages

Die Vereinbarung umfasst Tätigkeiten des ANs wie:

- Installation und Konfiguration von Hard- und Softwareprodukten
- Durchführung von Integrations- und Migrationsleistungen
- Fehleranalyse und Störungsbehebung
- Erbringung weiterer Supportleistungen zur Aufrechterhaltung des Betriebes
- Bereitstellung von SaaS-Anwendungen und Clouddiensten

Die für diesen Zweck zu verarbeitenden Daten sind wie folgt technologisch zu klassifizieren:

- Log- und Performancedaten
- Debugging-Daten
- Diagnose-Daten
- Profildaten von natürlichen und systemischen Identitäten
- Elektronische und physikalische Dateien
- Datenbankinformation

Von der Datenverarbeitung sind folgende Personenkreise betroffen:

- Mitarbeitende des AGs
- Geschäftspartner des AGs
- Studierende des AGs
- Besucher des AGs

# 3 Allgemeine Rechte und Pflichten des AGs

Der AG ist die verantwortliche Stelle im Sinne der gesetzlichen Rahmenbedingungen.

Der AG ist für die Wahrung der Betroffenenrechte definiert. Betroffenenrechte sind daher stets ihm geltend zu machen.

Der AN wird den AG unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte ihm gegenüber angezeigt haben.

Der AG hat das Recht, sich vor Beginn des Vertragsschlusses und in Folge regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit überzeugen zu können. Er kann diese Kontrolle auch durch einen Dritten durchführen lassen. Der AG wird das Ergebnis in geeigneter Weise dokumentieren.

Der AG hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Informationsverarbeitung gegenüber dem AN zu erteilen. Weisungen müssen ausschließlich in Textform erfolgen. Änderungen des Verfahrensgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

Der AG wird dem AN eine oder mehrere weisungsberechtigte Personen benennen. Für den Fall, dass sich die ändern oder längerfristig verhindert sind, wird der AG eine Vertretung dem AN in Textform mitteilen.

Der AG informiert den AN unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den AN feststellt.

Der AG bestimmt in Absprache mit dem AN den Zeitpunkt jeder Teleservice-Maßnahme. Zu diesem Zeitpunkt ermöglicht der AG dem AN Zugriff auf die betroffenen Systeme.

Vor Beginn des Fernzugriffs muss der AG diesem explizit zustimmen und beobachtet mit geeigneten Mitteln die vom AN durchgeführten Tätigkeiten. Der AG prüft das Wartungsprotokoll nach Erhalt und teilt dem AN auf Anforderung das Ergebnis der Prüfung.

Der AG hat das Recht, die Teleservice-Maßnahme jederzeit zu unterbrechen, insbesondere, wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Teleservice-Maßnahmen mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

# 4 Allgemeine Rechte und Pflichten des ANs

Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der vom AG erteilten ergänzenden Weisungen.

Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des AGs. Eine hiervon abweichende Verarbeitung von Daten ist dem AN untersagt, es sei denn, dass der AG dieser in der Textform zugestimmt hat.

Die Verarbeitung von Daten im Auftrag des AGs außerhalb der Betriebsstätten des ANs oder definierter Nachunternehmen ist nur mit Zustimmung des AGs zulässig. Diese ist in der Textform zu dokumentieren.

### 4.1.1 Gesetzliche Rahmenbedingungen

Der AN verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR) durchzuführen. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AGs.

Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Abschnitt 5.

### 4.1.2 Bestellung eines Datenschutzbeauftragten

Der AN bestätigt, dass er einen betrieblichen Datenschutzbeauftragten im Sinne des §4f BDSG bestellt hat und wird diesen gegenüber dem AG in Textform benennen. Die Pflicht zur Bestätigung kann im Ermessen des AGs entfallen, wenn der AN nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der AN nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verwendung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften sowie der Regelungen dieses Vertrages gewährleisten.

### 4.1.3 Organisationsverfahren

Der AN ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Informationen die er im Auftrag des AGs verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme durch Dritte geschützt sind.

### 4.1.4 Trennungsgebot

Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden (Trennungsgebot).

### 4.1.5 Informationspflichten

Der AN wird Änderungen in der Organisation die für die Sicherheit der Daten erheblich sind, vorab mit dem AG abstimmen. Soweit die beim AN getroffenen Sicherheitsmaßnahmen den Anforderungen des AGs nicht genügen, benachrichtigt er den AG unverzüglich.

Der AN wird die AG unverzüglich darüber informieren, wenn eine von dem AG erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der AN ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den AG bestätigt oder geändert wird.

Der AN ist verpflichtet, dem AG jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des AGs unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigte Personen erfolgt ist.

Der AN wird dem AG unverzüglich darüber informieren, wenn eine Datenschutzaufsichtsbehörde gegenüber dem AN tätig wird und dies auch eine Kontrolle der Verarbeitung, die der AN im Auftrag des AGs erbringt, betreffen kann.

Für den Fall, dass der AN feststellt oder Tatsachen die Annahme begründen, dass von ihm für den AG verarbeitete

- besondere Arten personenbezogener Daten
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der AN den AG unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls in Textform zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten.

Der AN ist verpflichtet unverzüglich mitzuteilen, welche Maßnahmen er getroffen hat, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Der AN verpflichtet sich, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem AG, insbesondere im Hinblick auf die Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den AG zu erteilen.

#### 4.1.6 Kennzeichnungspflicht

Der AN wird die Daten, die er im Auftrag für den AG verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der AN die Daten mit dem jeweiligen Zweck kennzeichnen.

#### 4.1.7 Löschung nicht mehr benötigter Unterlagen

Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den AG datenschutzgerecht vernichtet werden. Die Zustimmung bedarf der Textform.

### 4.1.8 Unterstützungsleistungen

An der Erstellung der Verfahrensakten und Verfahrensverzeichnisse durch den AG hat der AN mitzuwirken. Er hat dem AG die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

Der AN muss dem AG die Person(en) benennen, die zum Empfang von Weisungen des AGs berechtigt sind.

### 4.1.9 Durchführung von Teleservices

Der AN teilt dem AG vor Beginn von Teleservicemaßnahmen in der Textform mit, welche Mitarbeitende er dafür einsetzen wird und wie diese sich identifizieren werden. Die Mitarbeitenden des ANs verwenden hinreichend sichere Identifizierungsmaßnahmen.

Während der Teleservicemaßnahmen erstellt das Personal des ANs ein Protokoll aus dem die folgenden Informationen hervorgehen:

- Anfang und Ende der Teleservices,
- beteiligte Personen,
- betroffene Systeme und Netzwerkverbindungen,
- durchgeführte Tätigkeiten auf den einzelnen Systemen.

Die Protokolle werden dem AG unverzüglich nach Beendigung der jeweiligen Teleservice-Maßnahme auf Anforderung zur Verfügung gestellt.

Datenübertragungen zu Zwecken der Teleservices müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen und bedürfen der Zustimmung des AGs.

Wurden Daten des AGs im Zuge der Teleservices kopiert, so sind diese nach Abschluss der konkreten Servicemaßnahme unverzüglich zu löschen. Dies gilt nicht für Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Teleservices benötigt werden.

## 5 Unterauftragsverhältnisse

Die Beauftragung von Unterauftragnehmers (UA) durch den AN ist nur mit Zustimmung des AGs zulässig, die in der Textform erfolgen muss.

Der AN wird alle zum Vertragsschluss bestehenden Unterauftragsverhältnisse vor Aufnahme der Arbeiten in Textform mitteilen.

Der AN hat vor der Beauftragung zu prüfen, dass dieser die zwischen dem AG und AN getroffenen Vereinbarungen auch für seinen Leistungsbereich einhalten kann.

Der AN hat vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach den jeweiligen rechtlichen Grundlagen (z.B § 9 BDSG) und den Vereinbarungen dieses Vertrages erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom AN zu dokumentieren und auf Anfrage des AGs zu übermitteln.

Der AN ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten bestellt hat. Für den Fall, dass kein Datenschutzbeauftragter beim dem Unterauftragnehmer bestellt ist, hat der AN den AG hierauf hinzuweisen.

Der AN hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des AGs auch gegenüber den Unterauftragnehmern gelten. Der AN hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

Der AN hat mit dem Unterauftragnehmer einen Vertrag über die Verarbeitung personenbezogener Daten im Auftrag zu schließen, der den Voraussetzungen dieses Vertrages entspricht. Dem AG ist der entsprechende Vertrag auf Anfrage in Kopie zu übermitteln.

Der AN ist verpflichtet durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse dieses Vertrages des AGs oder der Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte vereinbart wurden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

Der AN ist verpflichtet auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zur gewährleisten.

Der AG ist berechtigt, eine Aufstellung aller Dienstleister, die Zutritt, Zugang oder Zugriff auf die im Auftrag zu verarbeitenden Daten bzw. Datenträger haben (können), zu erhalten und Einblick in die vertraglichen Regelungen zu nehmen.

Wartungs- und Prüfungsleistungen stellen stets zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen des AGs genutzt werden.

# 6 Herstellersupport Cisco Systems Inc.

Leistungen, die durch den Hersteller Cisco Systems direkt erbracht werden, werden durch den AG im Sinne dieser Informationssicherheitsrichtlinie als angemessen sicher anerkannt. Eine wesentliche Grundlage für diese Feststellung stellen die

„Binding Corporate Rules“

dar, in der sich der Hersteller zu einer angemessenen Einhaltung der gesetzlichen Anforderungen gemäß der EU-DSGVO verpflichtet. Eine gesonderte Bestätigung des AG zur Nutzung der Ressourcen des Herstellers muss daher seitens des ANs nicht beantragt werden.

# 7 Kontrollen

Der AG hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen Regelungen und Weisungen jederzeit im erforderlichen Umfang zu kontrollieren.

Die Durchführung und das Ergebnis der Kontrollen werden von dem AG in geeigneter Weise dokumentiert und dem AN auch Anforderung in Kopie übermittelt.

Der AN ist dem AG gegenüber zur Auskunftserteilung verpflichtet, soweit es zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

Der AG kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des ANs zu den jeweils üblichen Geschäftszeiten vornehmen. Der AG wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des ANs durch die Kontrollen nicht unverhältnismäßig zu stören.

Im Hinblick auf die Kontrollverpflichtungen des AGs stellt der AN vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags sicher, dass sich der AG von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierbei weist der AN dem AGs auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach, die aufgrund der gesetzlichen Grundlagen und dieser Vereinbarung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten erforderlich sind.

Er kann den Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren etc.) oder einer geeigneten Zertifizierung zum Datenschutz oder ein Datenschutzaudit erbringen.

Der AN akzeptiert das Kontrollrecht der zuständigen Behörden (z. B. Landeszentrums für Datenschutz), wenn aus konkretem Anlass eine Vor-Ort-Kontrolle unumgänglich ist. Dabei gewährt der AN auch Zugang zu den Rechenzentren, in denen die Daten des AGs verarbeitet werden. Werden diese durch einen oder mehrere Unterauftragnehmer betrieben, stellt der AN sicher, dass die zuständige Behörde zu den Rechenzentren der Unterauftragnehmer erhält. Ansonsten verpflichtet er sich, der Behörde direkt Auskunft zu erteilen, wenn diese unmittelbaren Bezug zur Auftragsdatenverarbeitung haben. Der AGs ist über entsprechende geplante Maßnahmen vom AN zu informieren.

## 8 Datengeheimnis

Der AN ist bei der Verarbeitung von Daten für den AG zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG verpflichtet. Der AN verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem AG obliegen. Der AG ist verpflichtet, dem AN etwaige besondere Geheimnisschutzregeln mitzuteilen.

Der AN sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der AN sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeitenden mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese schriftlich auf das Datengeheimnis im Sinne des § 5 BDSG verpflichtet werden. Sofern der AN im Zusammenhang mit Leistungen für den AG an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis im Sinne des § 88 Telekommunikationsgesetz zu verpflichten.

## 9 Geheimhaltungspflichten

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den oben genannten Zwecken zu nutzen oder diese Informationen Dritten zugänglich zu machen.

Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

## 10 Haftung

Der AN haftet gemäß EVB-IT Systemlieferungsvertrag gegenüber dem AG für Schäden, die der AN bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen.

Für den Ersatz von Schäden, die Betroffene wegen einer nach dem Gesetz oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der AG gegenüber den Betroffenen verantwortlich. Soweit der AG zum Schadensersatz gegenüber Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den AN vorbehalten.

Der AG haftet dem AN gegenüber nur für vorsätzliches oder grob fahrlässiges Verhalten. Diese Haftungsbeschränkung gilt nicht für Schäden aus der Verletzung des Lebens, Körpers oder der Gesundheit.

## 11 Vertragsdauer und Kündigung

Die Regelungen dieses Vertrages gelten für die Dauer des zwischen den Parteien geschlossenen Hauptvertrages sowie den in den Abrufaufträgen definierten Vertragsfristen, die über den Zeitraum der Rahmenvereinbarung hinaus bestehen können.

Der AG kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des AN gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der AN eine Weisung des AGs nicht erfüllen kann oder will oder der AN den Zutritt des AGs oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

## 12 Beendigung

Nach Beendigung des Vertrages hat der AN sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen. Die Datenträger sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen bei dem AN. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

Der AG hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim AN zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des ANs erfolgen. Die Vor-Ort-Kontrolle wird mit einer angemessenen Frist durch den AG angekündigt.

## 13 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechtes durch den Auftrag-nehmer im Sinne des § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen ist.

## 14 Schlussbestimmungen

Sollte das Eigentum des AGs beim AN durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch einen Insolvenzverwalter oder durch sonstige Ereignisse gefährdet werden, so hat der AN den AG unverzüglich zu informieren. Der AN wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

Sofern Regelungen dieses Vertrages von Bestimmungen des Hauptvertrages abweichen, gehen die Regelungen dieses Vertrages vor.

Nebenabreden zu diesem Vertrag bestehen nicht. Für Änderungen oder Ergänzungen ist die Schriftform erforderlich. Auf dieses Formerfordernis kann nur schriftlich verzichtet werden. Sollten einzelne Teile dieses Vertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Regelungen nicht.

Dieser Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft.

Erfüllungsort und Gerichtsstand für alle aus oder im Zusammenhang mit diesem Vertrag stehenden Streitigkeiten ist der Sitz des AGs.

# 15 TOM-Mindestanforderungen

Der AN verpflichtet sich gegenüber dem AG zur Einhaltung der technischen und organisatorischen Maßnahmen, die aufgrund der anzuwendenden Datenschutzvorschriften erforderlich sind. Nachfolgend werden unter den Punkten 15.1 bis 15.8 Mindestanforderungen dokumentiert, die der AN bei der Ausführung seiner Leistungen sicherstellen muss.

Der AN wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der AN den AG informieren, um die Anpassungen abzustimmen.

Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit, Verfügbarkeit, Transparenz, Nicht-Verkettbarkeit oder Intervenierbarkeit bei der Verarbeitung personenbezogener Daten beeinträchtigen können, wird der AN vorab mit dem AG abstimmen.

Maßnahmen, die lediglich geringfügige technische und organisatorische Änderungen mit sich bringen und die genannten Schutzziele nicht negativ beeinträchtigen, können vom AN ohne Abstimmung mit der AG umgesetzt werden. Der AG kann jederzeit eine aktuelle Fassung der vom AN getroffenen technischen und organisatorischen Maßnahmen anfordern.

## 15.1 Zutrittskontrolle

Definierte Mindestanforderungen:

- Gebäudesicherung über Alarmanlage
- Physisches Zugangskontrollsystem oder Sicherheitsschlösser
- Videoüberwachung der Zugänge
- Qualifizierte Regelung zur Schlüsselausgabe und -verwendung
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher und externer Unterauftragnehmer

## 15.2 Zugangskontrolle

Definierte Mindestanforderungen:

- Zentrale Zuordnung von Benutzerrechten und -profilen
- Authentifikation mit sicheren Verfahren
- Einsatz von VPN-Technologie
- Schlüsselregelung
- Sorgfältige Auswahl von Reinigungs- und Objektschutzpersonal
- Einsatz von Firewall und Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von mobilen Datenträgern mobilen Endgeräten

15.3 Zugriffskontrolle

Definierte Mindestanforderungen:

- Verwaltung der Rechte durch Systemadministrator
- Definition eines Berechtigungskonzepts
- Anzahl der Administratoren werden auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von mobilen Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

15.4 Weitergabekontrolle

Definierte Mindestanforderungen:

- Übertragung über sichere Standleitungen bzw. VPN-Tunneln (2048 Schlüssel)
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

15.5 Eingabekontrolle

Definierte Mindestanforderungen:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

15.6 Auftragskontrolle

Definierte Mindestanforderungen:

- Auswahl von Nachunternehmen unter Sorgfaltsgesichtspunkten insbesondere hinsichtlich der dort etablierten Maßnahmen zur Gewährleistung der Datensicherheit
- Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Schriftliche Weisungen an den AN zur Ausführung der Auftragsverarbeitung, der dieser Vereinbarung inhaltlich gleichsteht
- Verpflichtung der Mitarbeitenden des ANs auf das Datengeheimnis
- Die Rolle eines Datenschutzbeauftragten ist benannt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte wurden definiert und vereinbart

15.7 Verfügbarkeitskontrolle

Definierte Mindestanforderungen:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierte Serverräume inklusive Überwachung von Temperatur und Feuchtigkeit
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen
- Etabliertes Backup- & Recoverykonzept
- Vorhaltung eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

15.8 Trennungsgebot

Definierte Mindestanforderungen:

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Pseudonymisierte Daten durch Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsysteme