# Auftrag zur Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten

gemäß § 11 BDSG bzw. § 11 DSG.EKD

- nachstehend für das jeweils Zutreffende als DSG bezeichnet -

**zwischen**

.....

.....

.....

.....

- nachstehend als Auftraggeber bezeichnet -

**und der**

**HiOrg Server GmbH**
**Dr.-Schier-Str. 9**
**D-66386 St. Ingbert**

- nachstehend als Auftragnehmer bezeichnet -

- nachstehend einzeln oder gemeinsam auch (Vertrags-) Partei(en) genannt -

## *Präambel*

Die Vertragsparteien haben einen Vertrag über Zusammenarbeit „Nutzung HiOrg-Server“ geschlossen. Auf der Grundlage dieses Vertrages sind sie eine Vereinbarung eingegangen, die ein Auftragsdatenverarbeitungsverhältnis (gem. § 11 BDSG bzw. DSG.EKG) beinhaltet.

Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der Regelungen des § 11 DSG zu konkretisieren, schließen die Parteien die folgende Vereinbarung:

### 0. Grundsätze

Der Auftragnehmer ist verpflichtet, die Vertraulichkeit von Kundendaten zu wahren. Er ist insbesondere zur Einhaltung aller für den Datenschutz und die Datenverarbeitung geltenden Bestimmungen in der jeweils geltenden Fassung verpflichtet und wir die Einhaltung der einschlägigen Bestimmungen laufend überwachen.

Es sind die Regelungen des Bundes-Datenschutzgesetzes (BDSG) und des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG.EKD, sofern zutreffend) zu beachten.

Der Auftragnehmer wird die ihm zur Verfügung gestellten oder im Rahmen der Erfüllung der übertragenen Aufgaben bekannt gewordenen Daten des Auftraggebers ausschließlich auf der Basis dieses Vertrages und zur Erfüllung der übertragenen Aufgaben verwenden. Eine darüberhinausgehende Verarbeitung oder Nutzung der Daten des Auftraggebers zu anderen Zwecken ist ausdrücklich ausgeschlossen.

## 1. Gegenstand des Auftrags (§ 11 Abs. 2 S. 1 Nr. 1 BDSG)

Der Gegenstand des Auftrags ergibt sich aus dem ***Nutzungsvertrag HiOrg-Server, §1 Vertragsgegenstand,*** auf den hier verwiesen wird.

## 2. Dauer des Auftrags (§ 11 Abs. 2 S. 1 Nr. 1 BDSG)

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des ***Nutzungsvertrages HiOrg-Server, §3 Laufzeit, Kündigungsfristen***.

Eine vorzeitige Beendigung der Laufzeiten durch fristlose Kündigung ist im Falle einer Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen zulässig. Gleiches gilt, wenn der Auftragnehmer eine berechtigte Weisung des Auftraggebers nicht ausführen will oder kann.

Unabhängig von den vorstehenden Regelungen zu den Laufzeiten gelten die Verpflichtungen zum Datengeheimnis, die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Vertragsende hinaus.

## 3. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen (§ 11 Abs. 2 S. 1 Nr. 2 BDSG)

*Konkretisierung des Zwecks:*

Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber dient dem Zweck einer standortunabhängigen Planung, Alarmierung, Durchführung und Abrechnung von Veranstaltungen, Einsätzen oder Lehrgängen, sowie der Verwaltung benötigter materieller und personeller Ressourcen.

*Konkretisierung der Art:*

Zur Zweckerfüllung stellt der Auftragnehmer für den Auftraggeber das internetbasierte Datenbanksystem „HiOrg-Server“ mit der erforderlichen Hardware zum Betrieb der zentralen Datenbank und Webapplikation sowie deren Internetanbindung zur Verfügung***.***

*Konkretisierung des Umfangs:*

Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber umfasst die Speicherung und Verarbeitung im Datenbanksystem, die Verfügbarkeit über eine Internetanbindung sowie der Sicherung der Datenbestände***.***

*Konkretisierung der Art der Daten:*

Gegenstand der Erhebung, Verarbeitung und oder Nutzung personenbezogenen Daten sind folgende Datenarten /-kategorien:

- Name, Vorname, Alias, Passwort, Geburtsdatum und Wohnanschrift,
- Bankverbindung, Beruf, Arbeitgeber, Angehörige, Abwesenheitszeiten,
- Telefonnummern / Fax / E-Mail-Adresse, ggf. weitere Kontaktdaten,
- Foto, Fahrerlaubnis, Kleidergrößen, Ausbildung(en), Prüfungsdaten,
- Mitgliedschaftsdaten, Qualifikation, Dienststellung, Funktion,

- Einsatzzeiten, Einsatzorte, Aufgaben, persönliches Material und Dienstkleidung
- Ggf. weitere vom Auftragnehmer zusätzlich erfassten personenbezogene Daten (z.B. in dynamisch konfigurierbaren „benutzerdefinierten“ Datenfeldern)
- Lehrberechtigung, Kursteilnahme (bei Nutzung der Version „HiOrg-Server KURSE“)

*Konkretisierung zum Kreis der Betroffenen:*

Der Kreis der durch den Umgang ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Personal / Mitarbeiter des Auftraggebers
- Ansprechpartner, Veranstalter, Kunden, Geschäftspartner des Auftraggebers
- Kursteilnehmer, ggf. deren Arbeitgeber (bei Nutzung der Version „HiOrg-Server KURSE“)

## 4. Technische u. organisatorische Maßnahmen nach § 9 BDSG (§ 11 Abs. 2 S. 1 Nr. 3 BDSG)

Der Auftragnehmer gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung des Auftrags erforderlichen technischen und organisatorischen Maßnahmen gem. § 9 BDSG und Anlage. Der Auftragnehmer ermöglicht und unterstützt die Prüfung der Umsetzung der vereinbarten Maßnahmen vor Beginn sowie während der Verarbeitung durch den Auftraggeber.

Der Auftragnehmer hat die im Rahmen der Vertragsprüfung dargelegten, **nicht auftragsspezifischen**, technischen und organisatorischen umgesetzten Maßnahmen hinsichtlich der Zutrittskontrollen, Zugangskontrollen, Datenträgerkontrollen, Speicherkontrollen, Benutzerkontrollen, Zugriffskontrollen, Weitergabekontrollen, Eingabekontrollen, Ausgabekontrollen, Auftragskontrollen, Transportkontrollen, Verfügbarkeitskontrollen, Organisationskontrollen sowie des Trennungsgebots im Rahmen eines Selbstaudits vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben - **Anlage technische und organisatorische Maßnahmen zum Vertrag zur Auftragsdatenverarbeitung**. Die dokumentierten Maßnahmen werden Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Ergibt sich aus den Prüfungen Umsetzungsbedarf hinsichtlich der auftragsspezifischen vereinbarten Maßnahmen oder werden Änderungen der Maßnahmen aus anderen Gründen erforderlich, sind diese zunächst mit dem Auftraggeber abzustimmen. Die zu ergreifenden Maßnahmen können sich insbesondere auch aus konkreten Weisungen im Einzelfall des Auftraggebers ergeben.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG / § 21a DSG.EKD dem Auftraggeber zur Verfügung zu stellen.

## 5. Berichtigung, Löschung und Sperrung von Daten (§ 11 Abs. 2 S. 1 Nr. 4 BDSG)

Die Rechte der durch den Datenumgang beim Auftragnehmer betroffenen Personen insbesondere auf Berichtigung, Löschung und Sperrung sind gegenüber dem Auftraggeber geltend zu machen. Er ist allein verantwortlich für die Wahrung dieser Rechte.

Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

Der Auftragnehmer hat den Auftraggeber bei der Umsetzung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten zu unterstützen.

## 6. Pflichten des Auftragnehmers nach § 11 Abs. 4 BDSG (§ 11 Abs. 2 S. 1 Nr. 5 BDSG)

Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

Die Speicherung, Verarbeitung und Nutzung der Daten durch den Auftragnehmer findet ausschließlich im Gebiet der Bundesrepublik Deutschland 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. Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich.

Der Auftragnehmer ist verpflichtet, im Rahmen der Tätigkeit für den Auftraggeber sämtliche maßgeblichen datenschutzrechtlichen Bestimmungen, insbesondere diejenigen nach § 11 Abs. 4 BDSG sowie die Regelungen dieses Auftrags, einzuhalten. Er hat deren Einhaltung durch seine Mitarbeiter sicherzustellen und die Einhaltung regelmäßig zu kontrollieren. Dies gilt insbesondere für sämtliche Erhebungen, Verarbeitungen und / oder Nutzungen von personenbezogenen Daten, die der Auftragnehmer im Zusammenhang mit den vom Auftraggeber beauftragten Leistungen durchführt.

-- zu §§ 4f, 4g: --

Der Auftragnehmer sichert zu, dass er – soweit gesetzlich vorgeschrieben – einen/eine Datenschutzbeauftragte/n schriftlich bestellt hat, der seine Tätigkeit gemäß §§ 4f, 4g BDSG bzw. § 22 DSG.EKD ausüben kann. Er teilt dem Auftraggeber auf Anforderung dessen Kontaktdaten mit. Hinsichtlich des Auftrags kann sich der Auftraggeber direkt an den / die Datenschutzbeauftragte/n wenden.

Der Datenschutzbeauftragte des Auftragnehmers hat den Auftraggeber unverzüglich zu unterrichten, soweit er sich hinsichtlich dieses Auftrags auf das Zeugnisverweigerungsrecht bzw. auf das Beschlagnahmeverbot nach § 4f Abs. 4a BDSG beruft.

-- zu § 5: --

Der Auftragnehmer verpflichtet sich, beim auftragsgemäßen Umgang mit den personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 5 BDSG / § 6 DSG.EKD zu wahren.

Er hat hierzu beim Datenumgang ausschließlich Beschäftigte einzusetzen, die auf das Datengeheimnis verpflichtet sind und die sowohl hierüber als auch über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt wurden.

Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt wurden, die gesetzlichen Bestimmungen über den Datenschutz sowie die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten beachten.

-- zu § 9: --

Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung aller allgemeinen technischen und organisatorischen Maßnahmen entsprechend § 9 DSG und Anlage zu, um die Verpflichtungen gemäß dieser Vereinbarung einzuhalten bzw. deren Einhaltung sicherzustellen.

-- zu § 38: --

Der Auftragnehmer informiert den Auftraggeber unverzüglich, soweit eine Aufsichtsbehörde (auch) im Hinblick auf den Datenumgang im Rahmen dieses Auftrags beim Auftragnehmer im Rahmen ihrer Kompetenzen nach § 38 BDSG:

- Aufgrund eines Anlasses oder ohne konkreten Anlass prüft,
- Einen Verstoß beim Auftragnehmer zuständigen Stellen anzeigt,
- Betroffene über einen Verstoß unterrichtet,
- Auskunfts-, Zutritts- oder Einsichtsrechte beim Auftragnehmer ausübt,
- Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnet oder den Einsatz einzelner Verfahren beim Auftragnehmer untersagt.

Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.

## 7. **Kontrollpflichten des Auftragnehmers** (§ 11 Abs. 2 S. 1 Nr. 5 BDSG)

Der Auftragnehmer stellt im Rahmen seiner Verpflichtung zur Auftragskontrolle sicher, dass die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten im Auftrag des Auftraggebers nur entsprechend seinen Weisungen erfolgt. Hierzu führt er eine Kontrolle der Vertragsausführung bzw. -erfüllung durch. Diese bezieht sich insbesondere auf die Überwachung der Einhaltung von Regelungen und Maßnahmen zur Durchführung des Auftrags sowie die regelmäßige Prüfung und Anpassung der Wirksamkeit von Regelungen und Maßnahmen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu kann der Auftragnehmer bspw. die *Anlage technische und organisatorische Maßnahmen zum Vertrag zur Auftragsdatenverarbeitung*, IT-Sicherheits- oder Datenschutzaudits vorlegen.

Der Auftragnehmer unterstellt sich der Kontrolle durch den kirchlichen Datenschutzbeauftragten (§ 11 Abs. 5 DSG.EKD), sofern die Datenverarbeitung dessen Zuständigkeit unterliegt.

## 8. Berechtigung zur Begründung von Unterauftragsverhältnissen (§ 11 Abs. 2 S. 1 Nr. 6 BDSG)

Der Auftragnehmer ist zur Durchführung dieses Auftrags berechtigt, Unterauftragsverhältnisse für die Betreuung der physikalischen Hardware (Server) sowie deren redundanten Anbindung ans Internet über ein Rechenzentrum zu begründen.

Der Auftragnehmer informiert den Auftraggeber schriftlich, welche Unterauftragsverhältnisse er begründet hat, die den Kernbereich (Zweckbestimmung) dieses Auftrags berühren. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Die Einschaltung weiterer Unterauftragnehmer ist dabei auszuschließen.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 DSG i.V. mit Nr. 6 der Anlage zu §9 DSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Soweit dies im Falle der Unterauftragsverhältnisse mit einem Rechenzentrum nicht in vollem Umfang möglich ist, informiert der Auftragnehmer den Auftraggeber hierüber und übermittelt ihm die stattdessen zugrundeliegenden Vereinbarungen z. B. Allgemeine Geschäftsbedingungen (AGB) des Unterauftragnehmers.

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

## 9. Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungspflichten des Auftragnehmers (§ 11 Abs. 2 S. 1 Nr. 7 BDSG)

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 DSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung personenbezogener Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 DSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher,

dass der Auftraggeber sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 DSG und der Anlage durch Einsicht in ein im Hinblick auf den Auftrag umfassendes und aktuelles Datenschutz- und IT-Sicherheitskonzept nach.

Dabei kann der Nachweis für die Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage bspw. der *Anlage technische und organisatorische Maßnahmen zum Vertrag zur Auftragsdatenverarbeitung* oder eines IT-Sicherheits- oder Datenschutzaudits, den Datenschutzbeauftragten des Auftragnehmers oder einer Zertifizierung nach BSI-Grundschutz erbracht werden.

## 10. Mitteilungspflicht bei Verstößen des Auftragnehmers oder bei ihm beschäftigter Personen gegen Datenschutzvorschriften oder gegen den Auftrag (§ 11 Abs. 2 S. 1 Nr. 8 BDSG)

Stellt der Auftragnehmer fest, dass bei ihm gespeicherte personenbezogene Daten des Auftraggebers unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat er dies ohne Ansehen auf die Verursachung unverzüglich dem Auftraggeber mitzuteilen.

Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, beim Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

Der Auftragnehmer hat im Benehmen mit dem den Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergriffen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer hierbei zu unterstützen.

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

## 11. Weisungsbefugnisse des Auftraggebers (§ 11 Abs. 2 S. 1 Nr. 9 BDSG)

Für die Beurteilung der Zulässigkeit der Erhebung, Verarbeitung oder Nutzung sowie für die Wahrung der Rechte der Betroffenen insbesondere nach §§ 6, 7 und 8 DSG ist allein der Auftraggeber verantwortlich (§ 11 Abs.1). Der Auftraggeber ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Weisungen bedürfen der Schrift- oder Textform.

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (s.a. § 11 Abs. 3 BDSG). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

## 12. Rückgabe überlassener Datenträger (§ 11 Abs. 2 S. 1 Nr. 10 BDSG)

Eine Regelung nach Art der Dienstleistung ist nicht erforderlich bzw. möglich, da kein Austausch physischer Datenträger erfolgt.

## 13. Löschung nach Beendigung des Auftrags (§ 11 Abs. 2 S. 1 Nr.10 BDSG)

Bei Beendigung des Auftragsverhältnisses oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Erfolgt im Rahmen der Kündigung keine besondere Absprache, so wird der Auftragnehmer einen Monat nach Beendigung des Auftragsverhältnisses alle diesem Auftragsverhältnis zugeordneten Datenbestände löschen.

Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## 14. Hinweispflicht des Auftragnehmers (§ 11 Abs. 3 BDSG)

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Eine materiell rechtliche Prüfung steht dem Auftragnehmer nicht zu.

## 15. Haftung

Der Auftragnehmer ist verpflichtet, eine ausführliche Dokumentation der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu führen, anhand derer der Auftraggeber den Nachweis über deren Ordnungsmäßigkeit führen kann.

Auftragnehmer

_____

Ort, Datum


_____ _____

Auftraggeber

Ch. Blechschmitt
Geschäftsführer
HiOrg Server GmbH

Org.-Kürzel: _____

Anlage: Prüfliste der technischen und organisatorischen Maßnahmen gemäß §9 DSG

**Anlage technische und organisatorische Maßnahmen (TOM) zum Vertrag zur Auftragsdatenverarbeitung**

**Prüfliste der technischen und organisatorischen Maßnahmen**
gemäß §9 BDSG

## *A. Organisation*

Die innerbetriebliche Organisation ist durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

- ✓ schriftliche Arbeitsanweisungen, Richtlinien, Merkblätter
- ✓ Programme/Verfahren sind ordnungsgemäß dokumentiert
- ✓ Aufbewahrung maschinell erzeugter Protokolle/Logs ist geregelt
- ✓ Programmfreigabeverfahren ist eingerichtet
- ✓ Anwendung des Vier-Augen-Prinzip bei physikalischer Datenträgerzerstörung sowie bei weitreichenden Änderungen an Infrastruktur oder Software
- ✓ Benachrichtigungen, Auskunftsersuchen, Anliegen bzgl. Berichtigung, Löschung oder Sperrung werden dokumentiert
- ✓ Standort sämtlicher von der HiOrg Server GmbH genutzter Server: Deutschland

## *B. Sicherungsmaßnahmen*

Unsere Produktiv-Server für Intranet-System, Datenbank, sowie die Georedundanz werden in professionellen Rechenzentren in St. Ingbert bzw. München betrieben und gewartet.

**1. Zutrittskontrolle**

1.1. Der Zutritt zu DV-Systemen im Rechenzentrum wird Unbefugten verwehrt durch:
- Einteilung in Sicherheitszonen/Sperrbereiche
- Automatische Zutrittskontrolle
- Schlüsselregelung
- Personenkontrolle durch Pförtner

Das Rechenzentrum wurde in einem getrennten Bauabschnitt erstellt, als ECBS IT-Zelle / Raum-in-Raum-Lösung nach TIER-III-Standard (TÜV-zertifiziert)

1.2. Zutritt zum Rechenzentrum/Serverraum haben nur die jeweiligen Mitarbeiter, mit abgestuften Zutrittsregelungen

1.3. Nicht selbst zutrittsberechtigte Personen können die RZ-Räume nur nach Vor-abanmeldung und in Begleitung berechtigter Personen betreten

1.4. Die Zutrittskontrolle wird durch Alarmanlage und Gebäudebewachung unterstützt

## 2. Zugangskontrolle

2.1. Die unbefugte Nutzung der DV-Systeme wird verhindert durch Passwortvergabe und Protokollierung der Passwortnutzung
2.2. Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort
2.3. Über alle Aktivitäten auf der DV-Anlage werden automatisch Protokolle erstellt
2.4. Die Protokolle werden vom CSO oder der Geschäftsleitung mindestens wöchentlich, sowie bei Auffälligkeiten (z.B. besonders hohe Aktivität) ausgewertet
2.5. Die Datenübertragung von und zum DV-System wird bei kritischen Aktivitäten (z.B. Systempflege, Softwareupdates, Backup) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert:
- Standleitung / internes Netzwerk
- Teilnehmerkennung
- funktionelle Zuordnung einzelner Datenendgeräte
- Überprüfung bekannter öffentlicher Schlüssel bei Sitzungsbeginn
- verschlüsselte Datenübertragung (SSL / HTTPS / SFTP)
- Protokollierung der Systemnutzung und Protokollauswertung

## 3. Zugriffskontrolle

3.1. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern wird verhindert durch:
- Benennung eines Verantwortlichen für die Datenträger
- Bestandskontrolle
- kontrollierte Vernichtung (z.B. von Fehldrucken oder Datenträgern)

3.2. Die Datenträger werden auch außerhalb der Arbeitszeit an der Datenträgerverarbeitungsanlage aufbewahrt. Reine Backupmedien befinden sich in einem verschließbaren Schrank.
3.3. Es werden nur die für den jeweiligen Arbeitsplatz relevanten Datenträger dort vorgehalten. (Entwickler haben z.B. nur Zugriff auf fiktive Testdaten)
3.4. Die Datenträgerverwaltung wird nach vorgegebenem Schema (Dienstanweisung) durchgeführt.
- ausschließliche Nutzung festverbauter Datenträger (Festplatten)
- Protokollierung der produktiven und lagernden Bestände
- Ersatzteilbereitstellung durch das Rechenzentrum

3.5. Die Einschränkung der Zugriffsmöglichkeit des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:
- funktionelle Zuordnung einzelner Datenendgeräte
- automatische Prüfung der Zugriffsberechtigung
- Protokollierung der Systemnutzung und Protokollauswertung
- ausschließliche Menüsteuerung je nach Berechtigung
- differenzierte Zugriffsberechtigung auf Dateien/ Datensätze/ Datenfelder/ Anwendungsprogramme/ Betriebssystem
- differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen)

## 4. Weitergabekontrolle

4.1. Ein Versand von Datenträgern ist generell nicht vorgesehen
4.2. Es dürfen keine Behältnisse in die Serverräume oder in Datenträgerarchive mitgenommen werden, das Mitbringen privater Datenträger ist untersagt.
4.3. Nicht mehr benötigte magnetische Datenträger werden durch mehrfaches Überschreiben und anschließende physische Zerstörung durch eine Fremdfirma (auf

dem Gelände des Rechenzentrums) vernichtet.
Papierdatenträger werden mittels Reißwolf durch eine Fremdfirma auf dem Gelände des Rechenzentrums entsorgt.

4.4. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch:
- Standleitung
- SSL-Verschlüsselung der Datenübertragung
- Vollständigkeits- und Richtigkeitsüberprüfung
- Botentransport, verschlossen in Transportbehältnissen (nur im Ausnahmefall)

4.5. Es werden nur automatische, elektronische Empfangsbestätigungen eingesetzt.

4.6. Alle zum Transport vorgesehenen sensitiven Daten werden verschlüsselt.

4.7. Zur Weitergabe personenbezogener Daten werden folgende Dienste genutzt:
- E-Mail
- WWW (SSL), SFTP
- elektronischer Geldverkehr (SSL)

Folgende Sicherheitsmaßnahmen existieren:
- Hardware- und Software-Firewall
- Intrusion Detection System
- Virenschutzprogramme

4.8. An welchen Stellen Datenübermittlung durch Einrichtungen zur Datenübertragung vorgesehen ist, kann der Dokumentation der Übermittlungsstellen und -wege entnommen werden.

## 5. Eingabekontrolle

5.1. Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:
- Protokollierung eingegebener Daten
- Verarbeitungsprotokolle

## 6. Auftragskontrolle

6.1. Es existieren Verträge für folgende Formen der Auftragsdatenverarbeitung:
- Datenverarbeitung
- Datenträgervernichtung
- Wartung / Fernwartung
- Administration / Fernadministration

6.2. Die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers wird gewährleistet durch schriftliche Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragnehmer bzw. Rechenzentrum

6.3. Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor geplanten Wartungsfenstern oder gravierenden Änderungen; sämtliche Programmänderungen werden in einem Änderungslog veröffentlicht

6.4. Der Auftraggeber wird über Programmabbrüche und Programmfehler informiert

6.5. Sicherung der Fernwartung: entfällt, da keine Fernwartung beim Auftraggeber durch den Auftragnehmer vorgesehen

## 7. Verfügbarkeitskontrolle

7.1. Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch:

- Einsatz von RAID-Festplattensystemen bei allen Systemen
- mehrfach tägliche Backups von Software und Infrastruktur nach Backup-Plan
- Ablage der Backupdaten mehrfach und geographisch getrennt
- zusätzliche manuelle Backupmöglichkeit des Auftraggebers
- Storage Areal Network (SAN)
- Havariearchiv (Auslagerung)
- Unterbrechungsfreie Stromversorgung incl. Überspannungsfilter

7.2. Eine Planung für den Katastrophenfall liegt vor

7.3. Das System kann wahlweise in einem geographisch getrennten Rechenzentrum betrieben werden (Ausweich-Rechenzentrum)

## 8. Trennungsgebot

8.1. Dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, wird gewährleistet durch:
- softwareseitigen Ausschluss (Mandantentrennung)
- Dateiseparierung
- das Datenbankprinzip, Trennung über Zugriffsregelung
- Trennung von Test- und Produktionsprogrammen
- Trennung von Test- und Produktionsdaten
- Betrieb mehrerer getrennter Server für jeweils getrennte Aufgabenbereiche (Loadbalancer/Security/SSL, Webserver, Datenbankserver, Backupserver)

Stand der Information: 01.12.2011

Für die inhaltliche Richtigkeit:

Bereich Rechenzentrum

SKYWAY DataCenter GmbH
+49 (0) 6894 93 96 600 info@skyway-dc.com
www.skyway-dc.com

R. Schließmeyer
Geschäftsführer
SKYWAY DataCenter GmbH

Bereich Software / Intranet

HiOrg Server GmbH
Dr.-Schier-Str. 9
66386 St. Ingbert

C. Blechschmitt
Geschäftsführer
HiOrg Server GmbH