**Vereinbarung**
**zwischen Geschäftskunden**
**– nachfolgend „Auftraggeber“ genannt –**
**und der Uniscon GmbH**
**– nachfolgend „Auftragnehmer“ genannt –**
**betreffend der Nutzung des Dienstes iDGARD**

**Präambel**

Der Auftraggeber beabsichtigt, den Auftragnehmer im Rahmen der Erfüllung abgeschlossener und/oder noch abzuschließender Einzelverträge unter anderem auch mit der Verarbeitung personenbezogener Daten des Auftraggebers zu beauftragen. Mit dieser Vereinbarung sollen die datenschutzrechtlichen Rahmenbedingungen und diesbezüglichen Verpflichtungen der Vertragsparteien festgehalten werden, die im Zuge der zukünftigen Beauftragung unverändert Geltung beanspruchen. Diese Vereinbarung findet dabei Anwendung auf alle Tätigkeiten, die mit der Erfüllung des jeweiligen Einzelvertrages in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen oder kommen können. Diese Vereinbarung wird ergänzt durch konkrete, auftragsbezogene datenschutzrechtliche Regelungen, die jeweils in einem entsprechenden und auf diesen Auftrag Bezug nehmenden Einzelvertrag getroffen werden.

Diese Vereinbarung berücksichtigt insbesondere die Anforderungen nach § 11 Bundesdatenschutzgesetz (BDSG). Der Auftragnehmer hat mit der gebotenen Sorgfaltspflicht darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung von Aufträgen betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus dem Bereich des Auftraggebers erlangten Informationen, und zwar personenbezogene und sonstige Daten, nicht an Dritte weitergeben oder sonst verwerten.

Eine Besonderheit des Dienstes iDGARD ist, dass so genannte „**Betreibersicherheit**“ durch den Auftragnehmer geleistet wird. Der Aufbau der Systeme ist gemäß dem Prinzip der „**Sealed Cloud**“ gestaltet, das heißt, dass selbst bei Umgehung aller der in dieser Vereinbarung genannten technisch-organisatorischer Maßnahmen kein Zugriff auf die Daten im elektronisch, kryptographisch und mechanisch versiegelten Datenzentrum mit verhältnismäßigen Mitteln erfolgen kann. Einzelheiten zum Prinzip der Sealed Cloud sind auf der Internetseite www.idgard.de veröffentlicht.

Der Schutz durch die Versiegelung mittels Sealed Cloud betrifft die personenbezogenen Daten, die im Zusammenhang mit der Nutzung von iDGARD anfallen, einschließlich des Nutzernamens, des Passworts, und des „Passwort Unblocking Key“ (PUK) des Administrators, jedoch mit Ausnahme der Daten, die bei der Registrierung durch den Auftragnehmer erhoben werden und die zur Abrechnung der Dienstleistung erforderlich sind (z.B. Zahl der Lizenzen). Für alle Daten gelten aber mindestens die in dieser Vereinbarung genannten technisch-organisatorischen Maßnahmen.

Auch vom speziellen Schutz der Sealed Cloud umfasst sind die Daten, die für eine Wiederherstellung des Nutzerzugangs zu iDGARD bei verlorenem Nutzernamen oder Passwort und PUK des Administrators beim Auftraggeber erforderlich sind. Hierfür bietet iDGARD so genannte Treuhänder-Boxen.

Ebenfalls vom besonderen Schutz der Sealed Cloud umfasst sind die Verbindungsdaten, die für strafrechtliche Verfolgungen relevant sein könnten. Diese können durch die Vorrichtung „Sealed Freeze“ nur bei juristisch geprüft berechtigtem Interesse und nur von eigens dafür beauftragten Notaren gelesen werden.

Diese Vereinbarung ist gem. § 11 BDSG nur notwendig, wenn man juristisch den so genannten absoluten oder objektiven Personenbezug der personenbezogenen Daten zu Grunde legt. Vertritt man die Rechtsauffassung des relativen oder subjektiven Personenbezugs so ist diese Vereinbarung nicht notwendig, da die durch die Sealed Cloud geschützten Daten für den Auftragnehmer nicht personenbeziehbar sind.

**§ 1 Definitionen:**

(1) Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren 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. Unter Auftragsdatenverarbeitung im Sinne der vorliegenden Regelung wird auch die Erhebung oder sonstige Nutzung personenbezogener Daten gefasst.

(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 jeweiligen Einzelvertrag und diesen Rahmenvertrag festgelegt und können vom Auftraggeber danach durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

**§ 2 Gegenstand und Dauer des Auftrages**

Der Gegenstand und Dauer eines Auftrages ist in dem jeweiligen Einzelvertrag niedergelegt.

**§ 3 Umfang, Art und Zweck der Verarbeitung, Art der Daten und Kreis der Betroffenen**

Umfang, Art und Zweck der Verarbeitung sind ebenso wie die Art der Daten und der Kreis der Betroffenen gleichfalls in dem jeweiligen Einzelvertrag beschrieben. Ungeachtet des Vorstehenden, ist der Auftragnehmer zur Erfüllung des jeweiligen Vertragsgegenstandes unter Einhaltung der Bestimmungen dieser Vereinbarung und der Bestimmungen des jeweiligen Einzelvertrages zur Durchführung aller erforderlichen Verarbeitungsschritte und Nutzungen der vom Auftraggeber überlassenen sowie der ggf. für ihn erhobenen Daten (z.B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-files, Zwischendateien und Arbeitsbereichen etc.) berechtigt, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

Die Verarbeitung und Nutzung der Daten 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.

**§ 4 Weisungsgebundenheit des Auftragnehmers**

(1) Der Auftragnehmer verarbeitet oder nutzt die vom Auftraggeber überlassenen Daten ausschließlich im Rahmen der Bestimmungen dieser Vereinbarung, des jeweiligen Einzelvertrages und der speziellen Einzelweisungen des Auftraggebers. Gleiches gilt für das Erheben von Daten im Auftrag des Auftraggebers. Änderungen im Verfahrensablauf beim Auftragnehmer sind vorab mit dem Auftraggeber abzustimmen. Die Verarbeitung oder Nutzung der vom Auftraggeber überlassenen oder für den Auftraggeber erhobenen Daten zu anderen als den vertragsgegenständlichen Zwecken ist nicht gestattet.

(2) Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, ist er verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der vereinbarten Tätigkeit solange auszusetzen,

bis der Auftraggeber über das weitere Vorgehen entschieden hat.

**§ 5 Weitere Pflichten des Auftragnehmers**

(1) Der Auftragnehmer ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen. Geltenden Datenschutz-verordnungen und -rechten ist hierbei Sorge zu tragen.

(2) Der Auftragnehmer gewährleistet in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend § 9 Bundesdatenschutzgesetz. Insbesondere wird der Auftragnehmer 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, die den Forderungen des Bundesdatenschutzgesetzes entsprechen. Dies beinhaltet insbesondere

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zu-greifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- 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 Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- 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),
- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Nähere Einzelheiten zu denen vom Auftragnehmer getroffenen, technischen und organisatorischen Maßnahmen sind im Folgenden beschrieben:

A Zutrittskontrolle

Der Zutritt zu Datenverarbeitungs- und Telekommunikations-systemen wird Unbefugten durch folgende Maßnahmen verwehrt:

- Einteilung in Sicherheitszonen/Sperrbereiche
- Schlüsselregelung; Dokumentation
- Personenkontrolle durch den Rechenzentrumbetreiber incl. Dokumentation der Identitätspapiere bei jedem Zutritt
- Darüber hinaus findet grundsätzlich eine Begleitung durch eine neutrale, vom Datenzentrumbetreiber bestimmte Begleitperson statt
- Türen und Fenster des Datenzentrums sind einbruch- und alarmgesichert

Zutritt haben ausschließlich die für Wartungs- und Erweiterungsarbeiten beauftragten Mitarbeiter (abgestufte Zutrittsregelungen). Es besteht eine Liste zutrittsberechtigter Personen, deren Aktualisierungen schriftlich dokumentiert werden. Zudem findet grundsätzlich eine Begleitung durch eine neutrale, vom Datenzentrumsbetreiber bestimmte Begleitperson statt. Ein Zutritt wird nur unter Hinterlegung eines amtlichen Lichtbildausweises gewährt; die Dauer der Zutritte wird dokumentiert.

Für unternehmensfremde Personen und nicht zutrittsberechtigte Mitarbeiter muss eine schriftliche Einmalgenehmigung vorliegen. Der Zutritt wird mit Ausweiskontrolle und Anwesenheitsdauer protokolliert. Zu jeder Zeit muss mindestens eine zutrittsberechtigte Begleitperson anwesend sein.

Die Zutrittskontrolle wird durch folgende organisatorisch/ technischen Maßnahmen unterstützt:

- Alarmanlage
- Gebäudebewachung
- Videoüberwachung

B Zugangskontrolle

Die unbefugte Nutzung von Datenverarbeitungssystemen wird über die Vorrichtungen der Sealed Cloud hinaus durch folgende Maßnahmen verhindert:

- Passwörter
- Protokollierung der Passwortnutzung
- Passwort-Verwaltungssystem mit definiertem Rollenkonzept und Festlegung der Passwort-Policy

Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort. Die implementierte Password Policy ist noch schärfer ausgelegt, als die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen Parameter.

Für alle Administrator-Aktivitäten werden folgende Aufzeichnungen erstellt:

- Zutritt zum Datenzentrum
- Zugang zum System (s. Zugriffskontrolle)
- Durchgeführte Aktivitäten, komponentenbezogen
- Die Systemaktivitäten werden dokumentiert durch
  - System-Logs
  - System-Alarm-System
  - System-internes „Black-Box“-Gerät (WORM)

Diese Protokolle werden mindestens einmal im Monat ausgewertet. Bei Auffälligkeiten im Betrieb werden diese unmittelbar vom Sicherheitsverantwortlichen analysiert.

Zur Überwachung und Verhinderung von Zugriffen durch Unbefugte über das Netzwerk ist ein IDS (Intrusion Detection and Prevention System) implementiert, das über mehrere Stufen Firewall-Regeln umfasst sowie die bekannten Angriffe durch „Hacker“ abwehrt und protokolliert.

C Zugriffskontrolle

Die Einschränkung der Zugriffsmöglichkeit des zur Benutzung eines Datenverarbeitungs-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird durch folgende Maßnahmen gewährleistet:

- Der Zugriff auf Nutzerdaten ist durch die Sealed-Cloud-Technik bei iDGARD ausgeschlossen.
- Hintergründe zur Sealed-Cloud-Technik werden auf www.idgard.de vermittelt.
- A-rated SSL-Verschlüsselung (2048 bit Schlüssellänge) für die Übertragung vom Endgerät zur Sealed Cloud
- Alarmierung einer Man-in-the-middle-Attacke mit Browser-Plug-In möglich

- Kein Systemschlüssel; jeder Nutzersatz wird mit eigenem Schlüssel codiert, der aus Nutzername und Passwort generiert wird. Keine Speicherung dieser Schlüssel.
- AES-256 Verschlüsselung für jede Datei und jede Privacy Box separat.
- Keine dieser Schlüssel sind dem Betreiber der Cloud oder der Anwendung zugänglich.
- Komplette Neuverschlüsselung von Privacy Boxes, wenn diese geschlossen/versiegelt werden. Box-Links verlieren auch für Mitarbeiter des Dienstanbieters jede Missbrauchsmöglichkeit
- Unverschlüsselte Daten werden ausschließlich in den so genannten Data-Clean-Up Areas (ohne persistenen Speicher) verarbeitet
- Bei Alarm durch Sensorik auf logischer und physischer Ebene wird der so genannte Data Clean-Up ausgelöst.
- Der Data Clean-Up wird sowohl durch bei geplanten wie ungeplanten Zugriffsversuchen ausgelöst
- Hierfür werden zunächst die bestehenden Nutzersessions auf nicht betroffene Segmente der Sealed Cloud migriert und die unverschlüsselten Daten verschlüsselt und abgespeichert.
- Dann werden die Daten auf den Servern in den betroffenen Segmenten gelöscht und die Server ausgeschaltet.
- Durch einen stromlosen Zustand der Server von 15 Sekunden werden sicher alle unverschlüsselten Daten gelöscht bevor die eletro-mechanischen Türen den Zugriff auf die Server freigeben.
- HW-basierte „Chain of Trust“, die den gesamten Software-Stack umfasst.
- Entwicklungs- und Deploymentprozess mit signierten Software-Komponenten und –Versionen
- Zentrales Software-Deployment durch Net-Boot. Nur ein vollständig signierter Stack kann gebootet werden.
- Einsatz von mehrstufigen State-of-the-art Firewalls (klassisch mehrstufig und zusätzlich web application firewalls)
- Einsatz von State-of-the-art Systemen zur Intrusion Detection & Prevention
- Härtung der Server-Betriebssyteme
- Phyikalische Trennung der Netze zum Booting, Alarming und für Nutzlast
- Lastverteilung ohne Terminierung der Verschlüsselung
- Elektro-optische und elektro-mechanische Überwachung aller Systeme an Türen, Böden, Wänden und Deckeln
- Elektromechanische Schlösser steuern Zugriff gemäß der „Sealing Control“-Policy
- Aufzeichung aller Aktivitäten der Administratoren und Systemzustände (WORM-Technologie)
- Automatische Prüfung der Zugriffsberechtigung durch das System
- Festlegung der Zugriffe durch Password-Policy und Trennung der Systemkomponenten in verschiedene Segmente
- Trennung der Funktion „Zugriffsrechte zu erteilen“ und „Zugriff durchzuführen (Rollenkonzept, 4-Augen-Prinzip)
- Beschränkung der Fernwartungszugriffe; Konzept der Wartung hinsichtlich physischer und logischer Zugriffe
- Eine differenzierte Zugriffsberechtigung besteht für:
  - HW-Komponenten
  - Betriebssysteme
  - Serverspezifische Konfigurationen
  - Applikationen

Darüber hinaus wird laufend in Systembetrieb sowie bei Wartungs- und Updateaktivitäten die Integrität der Hardware- und Software-Komponenten geprüft. Insbesondere wird dadurch sichergestellt, dass Manipulation von Hardware ausgeschlossen ist und ausschließlich freigegebene Software installiert wird.

D Weitergabekontrolle

Daten werden, außerhalb des speziell gesicherten Verarbeitungsbereichs (Sealed-Cloud) grundsätzlich nur verschlüsselt gespeichert und ggf. übermittelt.

Es besteht ein Verbot der Mitnahme von Behältnissen in Räume mit Datenverarbeitungs-Anlagen oder in Datenträgerarchive. Zudem ist das Mitbringen privater Datenträger untersagt.

Nicht mehr benötigte Datenträger werden durch physische Zerstörung entsprechend DIN 66399/1-3 vernichtet.

Das unbefugte Lesen, Kopieren Verändern oder Entfernen von Daten bei der Übertragung sowie beim Transport von Datenträgern wird durch eine Datenverschlüsselung verhindert.

Für jede Übertragung bzw. Transport werden Empfangsbestätigungen, Lieferscheine o.ä. verwendet.

Zum Transport vorgesehene Daten mit sensitivem Inhalt (z.B. § 3 Abs. 9 bzw. § 42a BDSG) werden auf allen Datenträgern, Laptops und Datenübertragungsleitungen verschlüsselt.

Es existieren folgende Sicherheitsmaßnahmen:

- Firewall
- Virtual Private Networks (VPN)
- Content Filter

Neben den State-of-the-Art-Sicherheitsmaßnahmen geht die verwendete Sealed-Cloud-Technologie weit über die übliche Datensicherheit hinaus.

E Eingabekontrolle

Jede Eingabe, Veränderung, Löschung von Daten in Datenverarbeitungs-Systemen wird durch folgende Aufzeichnungen dokumentiert:

- Zutritt zum Datenzentrum
- Zugang zum System (s. Zugriffskontrolle)
- Durchgeführte Aktivitäten, komponentenbezogen
- Die Systemaktivitäten werden dokumentiert durch
  - System-Logs
  - System-Alarm-System
  - System-internes „Black-Box“-Gerät (WORM)

Der Auftraggeber wird über Programmabbrüche/ Programmfehler informiert.

F Auftragskontrolle

Im Zusammenhang mit den iDGARD Login-Cards besteht ein Unterauftragsverhältnis zur Datenverarbeitung, für das gemäß §11 BDSG eine schriftliche Vereinbarung getroffen wurde, obwohl lediglich die Verifikation eines Einmalpasswortes relativ zu einer pseudonymen Seriennummer einer iDGARD Login-Card vorgenommen wird. Dieser Unterauftragnehmer ist die Rempartec GmbH, HRB196973.

Ferner besteht mit der Contabo GmbH, HRB 180722 ein Auftragsverhältnis für zwei der Rechenzentren (eines in München, eines in Nürnberg), das allerdings nicht die Datenverarbeitung, sondern nur das „Housing“, d.h. die Bereitstellung von Räumlichkeiten, der Zutrittskontrolle hierzu und die Versorgung mit Strom, Kühlung, sowie den Netzanschluss betrifft.

G Verfügbarkeitskontrolle

Durch folgende Maßnahmen wird gewährleistet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsfilter
- Mehrfachredundanz der laufenden Systeme
- Kein Backup, um bei Löschungen eine echte und vollständige Löschung durchführen zu können.

Eine Planung für den Katastrophenfall ist vorhanden.

H Trennungskontrolle

Durch softwareseitigen Ausschluss (Mandantentrennung) und eine Separierung durch getrennte Verschlüsselung mit unterschiedlichen Schlüsseln wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

(3) Der Auftragnehmer ist verpflichtet, bei der Erhebung von Daten für den Auftraggeber sowie bei der Datenverarbeitung und -nutzung das Datengeheimnis gemäß § 5 BDSG zu wahren und ausschließlich Personal einzusetzen, das auf das

Datengeheimnis verpflichtet ist. Soweit andere Datenschutzgeheimnisse (Fernmeldegeheimnis, Sozialgeheimnis etc.) zu wahren sind, wird der Auftragnehmer seine Mitarbeiter entsprechend verpflichten.

(4) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer, das Ergebnis im Hinblick auf das Auftragsverhältnis dem Auftraggeber bekannt zu geben. Die im Prüfbericht der Aufsichtsbehörde feststellten Mängel wird der Auftragnehmer unverzüglich abstellen.

(5) Überlassene Datenträger (nur der Vollständigkeit halber, kommt bei der Nutzung von iDGARD nicht vor) 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. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Der Auftragnehmer stellt eine datenschutzkonforme Vernichtung von Test- und Ausschussmaterial sicher. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(6) 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 an den Daten beim Auftraggeber liegt.

(7) Die Auftragsdatenverarbeitung ist nur innerhalb der EU/des EWR zulässig. Für die Beauftragung von Subunternehmern gilt § 10 der vorliegenden Regelung.

(8) Die Umsetzung und Einhaltung der vereinbarten allgemeinen, technischen und organisatorischen Maßnahmen entsprechen der Schutzklasse III des Trusted Cloud Datenschutzprofils v.0.9 des Pilotprojekts Datenschutz-Zertifizierung für Cloud-Computing der Bundesregierung der Bundesrepublik Deutschland.

**§ 6 Zugriffsberechtigte Personen gemäß § 4 g (2) BDSG**

Aufgrund der Eigenschaft der Betreibersicherheit wie sie in § 4 und dort dem Abschnitt Zugriffskontrolle beschrieben ist, gibt es beim Dienst iDGARD keine zugriffsberechtigten Personen auf die Daten der Cloud-Nutzer.

**§ 7 Pflichten des Auftraggebers**

(1) Der Auftraggeber ist als verantwortliche Stelle Herr der Daten. Er ist 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.

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

(3) Der Auftraggeber wird dem Auftragnehmer seine anweisungs-, empfangs- und kontrollberechtigten Personen schriftlich oder im iDGARD-Registrierungsformular benennen.

(4) Der Auftraggeber verpflichtet sich, den Dienst erst in Anspruch zu nehmen, nachdem mit dem Auftragnehmer diese Vereinbarung schriftlich getroffen wurde.

**§ 8 Datenschutzbeauftragter des Auftragnehmers**

Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten seines betrieblichen Datenschutzbeauftragten mit:

Prof. Dr. Thomas Jäschke
DATATREE AG
Heubesstraße 10
40597 Düsseldorf
Tel. 0211-59894720

Der Datenschutzbeauftragte hat auf Seiten des Auftragnehmers auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften für den Datenschutz im Hinblick auf das Auftragsverhältnis hinzuwirken. Stellt der Datenschutzbeauftragte in diesem Zusammenhang Unregelmäßigkeiten fest, gilt § 5 Abs. 4 dieser Vereinbarung. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten des Auftragnehmers wenden.

Dem Auftraggeber werden durch den Auftragnehmer einmal jährlich, mindestens jedoch zum Jahresende auch die zusammenfassenden, relevanten Prüfberichte des Datenschutzbeauftragten des Auftragnehmers im Hinblick auf das Auftragsverhältnis zur Verfügung gestellt. Dieser Bericht umfasst auch die Unterauftragsverhältnisse und ggf. Änderungen, die Unterauftragsverhältnisse betreffen.

Sofern der Auftraggeber dem Einsatz von Subunternehmern gem. § 10 zugestimmt hat, erstreckt sich die jährliche Berichtspflicht auch auf die Einhaltung der bei den jeweiligen Sub-unternehmern einzuhaltenden technisch-organisatorischen Maßnahmen.

**§ 9 Rechte Betroffener; Berichtigung, Löschung und Sperrung von Daten**

Die Rechte der durch die Datenerhebung, -verarbeitung und -nutzung beim Auftragnehmer betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Er ist dabei insbesondere für die Benachrichtigung der Betroffenen (§ 33 BDSG), die Auskunftserteilung an die Betroffenen (§ 34 BDSG) sowie die Berichtigung, Löschung und Sperrung von Daten (§ 35 BDSG) verantwortlich. Der Auftraggeber wird den Auftragnehmer unverzüglich über die Berichtung, Löschung oder Sperrung von Daten informieren, sofern dies nicht selbstständig durch den Auftraggeber mit iDGARD erfolgen kann. Sollte sich ein Betroffener direkt an den Auftragnehmer wenden, so wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten. Im Übrigen hat der Auftragnehmer den Auftraggeber bei der Wahrung der Rechte Betroffener, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung, im Rahmen seiner Möglichkeiten zu unterstützen.

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 bereit zu stellen.

**§ 10 Kontrollrechte des Auftraggebers**

Der betriebliche Datenschutzbeauftragte des Auftraggebers oder die vom Auftraggeber nach § 6 Absatz 3 benannten Personen oder sonst vom Auftraggeber beauftragte Personen können sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

Der Auftragnehmer verpflichtet sich, dem betrieblichen Datenschutzbeauftragten des Auftraggebers oder den vom Auftraggeber nach § 6 Absatz 3 benannten Personen oder sonst vom Auftraggeber beauftragte Personen auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftrags-kontrolle erforderlich sind.

**§ 11 Subunternehmer**

Der Auftragnehmer ist nicht berechtigt, ohne die Zustimmung des Auftraggebers die Ausführungen der unter einem Einzelvertrag übergebenden Arbeiten ganz oder teilweise auf Subunternehmer zu übertragen. Soweit der Auftraggeber seine Zustimmung erteilt, sind die mit den Dritten zu treffenden Vereinbarungen schriftlich entsprechend so zu gestalten, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem betrieblichen Datenschutzbeauftragten des Auftraggebers, den vom Auftraggeber nach § 6 Absatz 3 benannten Personen oder sonst vom Auftraggeber beauftragte Personen sind Kontroll- und Überprüfungsrechte entsprechend § 9 einzuräumen.

Ebenso sind der betriebliche Datenschutzbeauftragte des Auftraggebers, die vom Auftraggeber nach § 6 Absatz 3 benannten Personen oder die sonst vom Auftraggeber beauftragten Personen berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

Der Auftragnehmer gewährleistet, dass nur solche Unterauftragnehmer einbezogen werden, die die Gewähr für die Einhaltung der datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung bieten und, dass der Unterauftragnehmer sich seinerseits davon überzeugt, dass seine Unter-Unterauftragnehmer die datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung erfüllen – mithin nicht ohne schriftlichen Auftrag agieren dürfen. Auch beinhaltet diese Gewährleistung, dass der Auftragnehmer sicherstellt, dass die Weisungen des Cloud-Nutzers an die Unter-Auftragnehmer und dessen Unter-Unterauftragnehmer weitergegeben und von diesen befolgt werden.

**§ 12 Rückgabe und Löschung von Daten bei Vertragsbeendigung**

Nach Beendigung des jeweiligen Einzelvertrages wird der Auftragnehmer die vom Auftraggeber überlassenen Daten sowie die für den Auftraggeber erhobenen, verarbeiteten und/oder genutzten Daten dem Auftraggeber herausgeben. Elektronisch gespeicherte Daten sind auf Wunsch des Auftraggebers entweder in einem marktüblichen Format auf elektronischen Datenträgern herauszugeben oder online zu übertragen.

Der Auftragnehmer wird sämtliche Daten, von denen der Auftraggeber keine Herausgabe wünscht, löschen bzw. vernichten und die Löschung/Vernichtung dem Auftraggeber schriftlich oder per E-Mail bestätigen. Dies gilt nicht für Schriftwechsel und für andere nach gesetzlichen Vorschriften aufzubewahrende Dokumente und Unterlagen oder zum Verbleib bei dem Auftragnehmer bestimmte Unterlagen. Weitergehende gesetzliche Löschungsverpflichtungen und Löschungsansprüche bleiben von vorstehenden Regelungen unberührt.

**§ 13 Schlussbestimmungen**

(1) Fügt der Auftragnehmer dem Auftraggeber unter einem Einzelvertrag durch eine vertrags- oder weisungswidrige Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers einen Schaden zu, ist er dem Auftraggeber zum Schadensersatz nach Maßgabe der gesetzlichen Bestimmungen verpflichtet.

(2) Änderungen und Ergänzungen dieser Vereinbarung, des jeweiligen Einzelvertrages und aller ihrer Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht.

Unterschrift Geschäftskunde (Auftraggeber)

(Ort, Datum, Unterschrift)

Unterschrift Uniscon GmbH (Auftragnehmer)

(Ort, Datum, Unterschrift)

Bitte senden Sie diese Vereinbarung unterschrieben im Doppel an: Uniscon universal identity control GmbH
Agnes-Pockels-Bogen 1
80992 München