CLOUD ADDENDUM

1. SCOPE

Dieses Cloud Addendum findet Anwendung auf die Zurverfügungstellung und Nutzung von MAPPs Cloud Software und ist im Zusammenhang mit dem sonstigen Vertrag zu lesen.

2. DEFINITIONS

2.1 „Cloud Software" meint sowohl SaaS als auch Hosted Software, aber nicht On-Premise Software.

2.2 „Verantwortliche Stelle" und "Auftragsdatenverarbeiter" sind zu verstehen wie von den jeweils anwendbaren Datenschutzgesetzen definiert.

2.3 „Finanzinformationen" meint alle Daten, die sich konkret auf Bankkonten, Kredit- und sonstige Zahlungskarten, Bonität/Ratings, Kontostände und andere finanzielle Fakten über eine Person oder Organisation beziehen und umfasst insbesondere alle Daten, die dem Payment Card Industry Data Security Standard (PCI DSS) unterliegen.

2.4 „Hosted Software" meint eine separate Einzelinstanz einer Software, die von MAPP gehosted und betrieben und nur vom Auftraggeber per Fernzugriff genutzt wird („Single-Tenant").

2.5 „SaaS" steht für „Software as a Service" und beschreibt das zentralisierte Hosting einer Software durch MAPP, die von mehreren Auftraggebern per Fernzugriff genutzt wird („Multi-Tenant").

2.6 „Planmäßige Softwarepflege" wird unter Ziffer 3.3 dieses Cloud Addendums definiert.

2.7 „Sensitive Daten" meint im Sinne des Artikel 8 der EU Richtlinie 95/46 Daten bezüglich der Rasse, ethnischer Herkunft, politischer Einstellung, religiöser oder philosophischer Ansichten, Gewerkschaftsmitgliedschaften, Gesundheit oder sexueller Orientierung.

3. ZURVERFÜGUNGSTELLUNG DER CLOUD SOFTWARE

3.1 MAPP stellt dem Auftraggeber die Cloud Software zum Fernzugriff in einer sicheren Systemumgebung zur Verfügung. Eine Überlassung der Cloud Software an den Auftraggeber findet nicht statt. Für die Nutzung der Cloud Software benötigt der Auftraggeber einen Standardwebbrowser entsprechend der „MAPP Supported Platform Matrix", die auf Anfrage zur Verfügung gestellt wird. MAPP wird sich bei der Zurverfügungstellung der Cloud Software an den Auftraggeber an alle auf MAPP als Auftragsdatenverarbeiter anwendbaren Gesetze und Regelungen halten.

3.2 Der Zugriff auf und die Nutzung der Cloud Software ist begrenzt entsprechend der vertraglichen Regelungen (z.B. hinsichtlich des verfügbaren Speicherplatzes, der Rechenleistung, der Anzahl der Nutzer). Diese vertraglichen Begrenzungen dürfen bei der Nutzung der Cloud Software durch den Auftrageber nicht überschritten werden.

3.3 MAPP führt regelmäßig planmäßige Softwarepflegeleistungen an der Software durch. Während dieser Softwarepflegeleistungen kann es zu einer eingeschränkter Verfügbarkeit oder Nichtverfügbarkeit der Software kommen. Über solche geplanten Routinewartungen am System wird MAPP den Auftraggeber rechtzeitig per E-Mail und/oder über das T@YS (MAPP At Your Service) Portal informieren (mindestens 24 Stunden vor dem geplanten Beginn der Softwarepflegeleistung). MAPP wird dabei wirtschaftlich angemessene Anstrengungen unternehmen, um solche Softwarepflegeleistungen außerhalb der Kerngeschäftszeiten (Werktags von 9 – 18 Uhr) durchzuführen. Der Umfang der geplanten Routinewartungen wird acht Stunden pro Kalendermonat nicht überschreiten.

3.4 Soweit vertraglich nicht ausdrücklich anderweitig vereinbart hat der Auftraggeber keinen Anspruch auf eine eigene IP-Adresse aus MAPPs IP-Adress-Pool, einen eigenen physischen Server oder eine dedizierte Übertragungskapazität und Bandbreite.

3.5 Der Auftraggeber erkennt an, dass die Übertragung von Daten über das Internet spezifische Risiken mit sich bringt und dass dabei unbefugte Zugriffe Dritter nicht mit absoluter Sicherheit zu verhindern sind. MAPP haftet nicht für Datenverluste oder Datenveränderungen während bzw. aufgrund einer Übertragung über das Internet. Der Auftraggeber ist verantwortlich für Zugriffe Dritter auf die Cloud Software mittels unbefugter Nutzung der Logins/Passwörter des Auftraggebers. Der Auftraggeber ist sich bewusst, dass es zu unberechtigten Zugriffen auf die Cloud Software kommen kann, etwa durch Hacking und nicht autorisierte Nutzung von Passwörtern oder Logins. Die Sicherheit der erteilten Logins und Passwörter obliegt allein dem Auftraggeber und seinen Nutzer.

3.6 In Übereinstimmung mit MAPPs jeweils aktuellen Backup-Policies erstellt MAPP regelmäßig Sicherungskopien (Backups) des Systems des Auftraggebers, um eine ordnungsgemäße Datenverarbeitung zu gewährleisten

(Verfügbarkeitskontrolle). MAPP behält es sich vor, die Backup-Policies in Ausübung pflichtgemäßen Ermessens anzupassen, beispielsweise um der technischen Entwicklung Rechnung zu tragen.

3.7 MAPP setzt weltweite Expertenteams und Ressourcen ein, um die vertragsgegenständlichen Leistungen für den Auftraggeber zu erbringen. MAPP ist dementsprechend berechtigt, die Cloud Software und jede Art von Daten (inklusive personenbezogener Daten), die mittels der Cloud Software verarbeitet werden, weltweit zu speichern/hosten und auf die Cloud Software bzw. auf die mit ihr verarbeiteten Daten weltweit, auch aus anderen Ländern als dem Sitzland des Auftraggebers und/oder von MAPP, zuzugreifen.

3.8 MAPP ist berechtigt, aber nicht verpflichtet, auf die Cloud Software zuzugreifen und Diagnose- und Analyseprogramme anzuwenden, um (i) die Einstellungen der Cloud Software anzupassen, um die Leistung und/oder Sicherheit der Cloud Software zu verbessern, vorausgesetzt dass diese Anpassungen keine negativen Auswirkungen auf die Nutzung der Cloud Software durch den Auftraggeber haben; (ii) Systemdaten (keine personenbezogenen Daten) über die Nutzung der Cloud Software zu erheben, um diese im Rahmen der Identifikation und Behebung potentieller Mängel und Fehler der Cloud Software zu nutzen; (iii) statistische Analysen zu erstellen und (iv) Forschung und Entwicklung zu unterstützen.

4. NUTZUNG DER CLOUD SOFTWARE

4.1 Der Auftraggeber hat sich bei der Nutzung der Software, inklusive verbundener Dienstleistungen, wie das Website Hosting, dem Versand von Nachrichten und der Datenverarbeitung durch die Software an die jeweils anwendbaren rechtlichen Vorschriften zu halten. Der Auftraggeber ist hierbei allein verantwortlich, sich über das jeweils geltende Recht, dessen Auslegung und Anwendung sowie die anwendbaren Industriestandards zu informieren und diese einzuhalten. Hierzu kann es notwendig sein, dass der Auftraggeber die Voreinstellungen der Software verändern muss.

4.2 Der Auftraggeber darf die Cloud Software nur zu eigenen Zwecken (Internal Use) nutzen und darf (i) sie nicht für die Verarbeitung von rechtsverletzenden, sittenwidrige, bedrohende, beleidigende oder sonst unrechtmäßigen oder unerlaubten Inhalten verwenden, dies umfasst SPAM, jugendbedrohliches Material oder Inhalte, die Rechte Dritter verletzen können; (ii) mit der Software nichts verarbeiten, was Viren, Würmer, Trojaner oder andere Schadsoftware oder schädliche Codes, Dateien, Skripte oder sonstige Programme enthält; (iii) nicht wissentlich die Integrität oder Performance der Cloud Software beeinflussen oder stören; oder (iv) versuchen, unerlaubt Zugang zur Cloud Software oder den verbundenen Systemen oder Netzwerken zu erhalten. MAPP ist berechtigt, Material oder Inhalte zu entfernen, von denen MAPP annehmen muss, dass sie gegen diese Vorschrift verstoßen.

4.3 Der Auftraggeber hat für eine sichere Verbindung zu sorgen, um die Cloud Software zu nutzen oder Daten dorthin zu übertragen. Um die Geheimhaltung und Integrität der Daten des Aufraggebers zu gewährleisten, welche von der Software gehosted und/oder verarbeitet wird, hat der Auftraggeber die ihm zur Verfügung gestellten Zugangsdaten nach Erhalt zu ändern und geheim zu halten. Die gewählten Zugangsdaten haben dabei hinsichtlich Komplexität und Änderungsintervall den Standards der jeweils gültigen MAPP Passwort Policy zu entsprechen, welche auf Aufforderung hin vorgelegt wird. Zugangsdaten dürfen nicht an Dritte weitergegeben werden. Gemeinschaftszugänge sind nicht gestattet. Der Auftraggeber hat MAPP unverzüglich über den Verlust oder die Bekanntgabe von Zugangsdaten zu informieren oder, wenn ein spezieller Zugang nicht länger benötigt wird.

4.4 Der Auftraggeber darf keine sensitiven Daten und Finanzinformationen mit der Cloud Software speichern und/oder verarbeiten.

4.5 Für alle Daten, die MAPP zur Verfügung gestellt werden, muss der Auftraggeber regelmäßig und risikoadäquat Sicherungskopien anfertigen und aufbewahren.

4.6 Der Auftraggeber ist allein verantwortlich für:

a) jede Art von Schaden, welche an Daten des Auftraggebers oder der Software durch fahrlässiges oder vorsätzliches Verhalten der Angestellten oder Erfüllungsgehilfen des Auftraggebers verursacht werden;
b) das Verhalten von Dritten, welche sich durch Nutzung der Zugangsdaten des Auftraggebers ohne Zutun MAPPs Zugang zur Software verschafft haben;
c) die Einhaltung aller für die Tätigkeit des Auftraggebers relevanten rechtlichen Vorgaben;
d) angemessene Sicherheitsprozesse, Hilfsmittel und Kontrollen für das System und Computernetzwerk, mittels derer der Auftraggeber auf die Cloud Software zugreift;
e) die eigene Auswahl von Sicherheitskopien, alternative Speichermöglichkeiten und Business Prozesse für den Fall, dass die Cloud Software nicht verfügbar ist und
f) die Bestimmung der Sicherheit, des Datenschutzes und der Backupeinrichtungen, welche für den Geschäftsbetrieb des Auftraggebers notwendig sind und hinsichtlich der Pflichten des Datenschutzes.

4.7 Der Auftraggeber hat sicherzustellen, dass MAPPs technische und organisatorische Maßnahmen und Sicherheitskontrollen den Ansprüchen des Auftraggebers entspricht und die notwendigen Verpflichtungen des Auftraggebers erfüllen, um seine Daten hinreichend zu schützen.

5. VERFÜGBARKEIT

5.1 MAPP wird wirtschaftlich angemessene Anstrengungen unternehmen, um dem Auftraggeber die Software 24 Stunden am Tag, 7 Tage die Woche, zur Verfügung zu stellen. MAPP wird dem Auftraggeber die Software mit einer Verfügbarkeit von mindestens 99 % des jeweiligen Kalendermonats zur Verfügung stellen (nachfolgend „Mindestverfügbarkeit").

Verfügbar ist die Software in diesem Zusammenhang, wenn zwischen den Servern, auf denen die Software gehostet wird, und dem Übergabepunkt zum Internet eine ununterbrochene Verbindung besteht und der Auftraggeber in der Lage ist, sich anzumelden und Zugriff auf die Software hat. Die Mindestverfügbarkeit bezieht sich nicht auf Test- und Entwicklungsserver.

5.2 MAPP misst die Verfügbarkeit anhand einer Testseite innerhalb der Software in regelmäßigen Abständen. Der Prozentsatz der Verfügbarkeit in einem Kalendermonat wird berechnet, indem die Anzahl der erfolgreichen Verfügbarkeitsmessungen (Testseite verfügbar) durch die Gesamtzahl der Verfügbarkeitsmessungen des jeweiligen Kalendermonats, abzüglich der Ausschlusszeiten (wie unten definiert), geteilt wird. Die Verfügbarkeitsmessung wird von MAPP ausgeführt und ist für diesen Vertrag maßgeblich. Die Ergebnisse der Messungen werden dem Auftraggeber auf Anfrage hin mitgeteilt.

Als Ausschlusszeiten werden solche Zeiten gerechnet, zu denen die Software aus nachfolgenden Gründen nicht verfügbar ist:

- Planmäßige Softwarepflege;
- Ausfälle und Verfügbarkeitsunterbrechungen, die durch den Auftraggeber oder einen Dritten verursacht werden, soweit es sich bei dem Dritten nicht um einen von MAPP eingesetzten Subunternehmer handelt, und/oder
- Ausfälle und Verfügbarkeitsunterbrechungen, die durch höhere Gewalt verursacht wurden und von MAPP nicht zu vertreten sind.

5.3 Sollte die Verfügbarkeit innerhalb eines Kalendermonats unter die Mindestverfügbarkeit fallen, so hat der Auftraggeber Anspruch auf eine Gutschrift. Die Höhe der Gutschrift beträgt 1°% der geschuldeten Lizenz-/Nutzungsgebühren für die Software für den betroffenen Monat für jedes Promille, um das die Mindestverfügbarkeit unterschritten wird. Die Gutschrift ist hierbei auf maximal 25 % der geschuldeten Lizenz-/Nutzungsbühren für den betroffenen Kalendermonat begrenzt. Eine Gutschrift wird mit nachfolgenden Rechnungen verrechnet und kann nicht ausgezahlt werden. Etwaige ausstehende Gutschriften verfallen mit Ende des Vertrages. Eine Gutschrift wird nur erstellt, wenn der Auftraggeber eine solche innerhalb von zwei Monaten ab dem Ende des betroffenen Kalendermonats beantragt.

5.4 Der Auftraggeber erkennt an, dass die in diesem Cloud Addendum vereinbarten Kompensationen/Gutschriften für den Fall der Unterschreitungen der Mindestverfügbarkeit eine angemessene Schätzung der Schäden, die der Auftraggeber voraussichtlich aufgrund einer Unterschreitung der Mindestverfügbarkeit erleiden würde, und dementsprechend auch eine angemessen Kompensation darstellen. Dementsprechend regelt dieses Cloud Addendum die Ansprüche des Auftraggebers gegen MAPP für den Fall einer Unterschreitung der Mindestverfügbarkeit abschließend und weitere Schadensersatzansprüche sind ausgeschlossen.

6. DATENSCHUTZ

6.1 MAPP verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich gemäß der vertraglichen Vereinbarungen und gemäß der Weisungen des Auftraggebers. MAPP wird die personenbezogenen Daten des Auftraggebers nicht für eigene Zwecke verarbeiten. Bei der Nutzung der Cloud Software ist der Auftraggeber stets als verantwortliche Stelle und MAPP als Auftragsdatenverarbeiter anzusehen.

6.2 Auftraggeber und MAPP verantworten unabhängig voneinander die Einhaltung der für sie jeweils anwendbaren Datenschutzbestimmungen. Der Auftraggeber wird MAPP die zur Erfüllung der vertraglichen Pflichten von MAPP erforderlichen Weisungen erteilen. Der Auftraggeber bestimmt durch seine Weisungen den Umfang der durch MAPP zu verarbeitenden Daten. Daher übernimmt MAPP keine Haftung für Ansprüche von betroffenen Personen, welche sich gegen eine Handlung oder Unterlassen von MAPP richten, soweit MAPP diese aufgrund von Weisungen durch den Auftraggeber durchgeführt hat. Unabhängig davon ist MAPP nicht verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, wenn dies zusätzliche Dienstleistungen oder zusätzliche Ausgaben bedeuten würde, es sei denn, der Auftraggeber hat einer Übernahme der Kosten zugestimmt.

6.3 Die Auftragsdatenverarbeitung umfasst die in diesem Vertrag spezifizierten Tätigkeiten. MAPP sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die zu treffenden Maßnahmen beinhalten insbesondere:

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet 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 personenbezogenen Daten des Auftraggebers zugreifen können, und dass personenbezogene Daten des Auftraggebers 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 des Auftraggebers 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 des Auftraggebers 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 des Auftraggebers in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle);

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

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

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten des Auftraggebers getrennt verarbeitet werden können (Trennungskontrolle).

Weitere Einzelheiten werden bei Bedarf vorgelegt. Der Auftraggeber hat sicherzustellen, dass die getroffenen Maßnahmen den individuellen Bedürfnissen hinsichtlich der Sensitivität, Geheimhaltung und Sensibilität der von MAPP zu verarbeitenden Daten entsprechen.

6.4 Jede Vertragspartei wird die andere Partei so schnell wie möglich über einen Bruch der Datensicherheit informieren, soweit Daten des Auftraggebers betroffen sind. Die Parteien werden sich abstimmen, um einen solchen Bruch zu untersuchen. MAPP wird in einer vernünftigen Weise mit dem Auftraggeber kooperieren, um dem Auftraggeber die Aufklärung zu ermöglichen. Dies schließt unter anderem ein, (i) den Auftraggeber bei den Untersuchungen zu unterstützen, (ii) ihm Zutritt zu betroffenen Räumlichkeiten zu gestatten, (iii) Befragungen von Angestellten von MAPP oder anderen, mit dem Bruch in Verbindung stehenden Personen, (iv) alle relevanten Unterlagen, Aufzeichnungen, Dateien, Reports und andere Materialien bereit zu stellen, welche gemäß Gesetz, Regulierungen und Industriestandards offenzulegen sind. Jede Partei wird so schnell wie sinnvollerweise möglich alle erforderlichen Maßnahmen treffen, um eine Wiederholung des Sicherheitsbruches zu verhindern.

6.5 Auf schriftliche Aufforderung des Auftraggebers, allerdings nicht häufiger als einmal pro Kalenderjahr, hat MAPP einen Fragebogen des Auftraggebers zu MAPPs Informationssicherheit und Maßnahmen zum Datenschutz wahrheitsgemäß zu beantworten. Nach der Kontrolle des Fragebogens hat der Auftraggeber die Möglichkeit, die Angaben durch ein Audit zu überprüfen. Hierzu ist eine entsprechende Anfrage von mindestens vier Wochen vor dem geplanten Audit an MAPP zu stellen. Dabei darf das Audit nicht länger als einen (1) Arbeitstag während MAPPs üblicher Geschäftszeiten in Anspruch nehmen und ist gemäß eines gemeinsam festzulegenden Ablaufes so durchzuführen, dass das Audit einen möglichst geringen Einfluss auf die Produktivität von MAPP darstellt. Der Auftraggeber kann maximal alle fünf Kalenderjahre ein Audit durchführen, es sei denn, ein Audit oder ein Fragebogen offenbart einen Verstoß gegen die Maßgaben dieses Vertrages hinsichtlich des Datenschutzes und der Informationssicherheit. Hinsichtlich eines Audits haben sich Auditoren und Auftraggeber an die Sicherheitsbestimmungen von MAPP zu halten. MAPP behält sich das Recht vor, dem Auftraggeber Arbeit und Zeitaufwand in angemessenem Umfang in Rechnung zu stellen, soweit das Audit die von MAPP genehmigte Dauer übersteigt.

6.6 Sollte eine staatliche Behörde die Offenlegung von Kundendaten verlangen, welche durch MAPP im Auftrag des Auftraggebers gespeichert werden, wird MAPP versuchen, die Behörde zunächst an den Auftraggeber zu verweisen. Sollte MAPP dennoch verpflichtet sein, die Anfrage der Behörde zu beantworten, wird MAPP, soweit rechtlich zulässig, zumutbare Anstrengungen unternehmen, den Auftraggeber hierüber zu informieren und die Offenlegung auf solche Daten beschränken, deren Offenlegung rechtlich notwendig ist.