Gültig ab dem 01.03.2015

FACTSHEET HCM CLOUD

Sicherheit, technische Daten, SLA, Optionen

1. Sicherheit und Datenschutz

Wo befinden sich meine Daten?

Zugegeben - der Begriff Cloud kann Unbehagen auslösen; impliziert er doch, dass Daten „irgendwo in der Cloud" herumschwirren. Für den Anwender ist unklar, wo genau sich seine Daten befinden, denn physisch ist der Standort „Cloud" oder „Wolke" zugegebenermaßen nur schwer auszumachen.

Wir möchten Ihnen diese Unsicherheit nehmen, und in diesem Paper transparent darstellen, wo sich Ihre Daten befinden, und was für ihre Sicherheit und Verfügbarkeit getan wird.

Beschreibung des Rechenzentrums

Standort des Rechenzentrums
>> Deutschland, Limburgerhof

Befindet sich das Rechenzentrum in einem gefährdeten Gebiet (Überflutung, Erdbeben)?
>> Nein

Gibt es im Rechenzentrum eine redundante Stromversorgung, eine unterbrechungsfreie Stromversorgung (USV) oder Generatoren?
>> Ja, USV- und Diesel-Generator

Ist im Rechenzentrum eine Notstromversorgung installiert? Gibt es eine Notbeleuchtung
>> Ja und ja

Wird mit mehr als einem Netzwerkbetreiber zusammengearbeitet?
>> Ja.

Ist die Anlage skalierbar?
>> Ja. Nach oben sind keine Grenzen gesetzt.

Datensicherheit im Rechenzentrum

Wird das Rechenzentrum mit einer Zugangskontrolle (Ausweis und/oder biometrische Daten) gesichert?
>> Ja, die Zugangskontrolle ist chipbasiert

Wer hat Zutritt zum Rechenzentrum?
>> Nur überprüfte und zugelassene Mitarbeiter

Wird das Rechenzentrum mit Hilfe von Kameras überwacht?
>> Ja, der komplette Außenbereich wird von Kameras überwacht

Ist der Zugriff auf Kundendaten im Rechenzentrum beschränkt?
>> Ja, es gibt keinen Zugriff auf Kundendaten

Sind für den Fall von Verletzungen der Datensicherheit entsprechende Untersuchungen vorgesehen?
>> Ja.

Wird die Verarbeitungsumgebung überwacht?
>> Ja.

Datenschutz

Alle Daten und Zugriffe sind durch ein Rechte- und Zugriffskonzept geschützt, d.h. es wird individuell konfiguriert, wer was im System bearbeiten und sehen darf. Dies gilt für den Zugriff auf Vorgänge und damit auch auf die eingegeben Daten und die konfigurierten Ansichten. Auch die Portaloberfläche kann individuell konfiguriert werden. Grundsätzlich werden im System keine personenbezogenen Daten gehalten. Dies wäre nur der Fall, wenn z.B. das System für ein Personalmanagement genutzt werden würde, d.h. wenn Anwendungen konfiguriert werden, die entsprechende personenbezogene Daten beinhalten. Das System verlangt jedoch immer eine bewusste Freigabe, sodass die Einstellung definiert vorgenommen werden muss.

Ist das Rechenzentrum zertifiziert?
>> Ja, nach ISO 27001

Ist ein Datenschutzbeauftragter im Rechenzentrum bestellt?
>> Ja, nach §4f BDSG

Steht eine Firewall zur Verfügung?
>> Ja

Wird eine Internet Security Software eingesetzt?
>> Ja

Wie wird die Sicherung der Installation durchgeführt?
>> Imagesicherung der kompletten Virtuellen Maschine auf externes Storage 5x pro Woche

Wie erfolgt der Zugriff auf die Lösung durch den Kunden?
>> 256 Bit SSL für verschlüsselten Zugriff auf die Anwendung

Datenübertragung

Die Übertragung der Daten erfolgt auf Gefahr des Kunden über das Internet ohne Gewähr von HCM. Die Mitteilungen sind nach deren Eingang gültig und werden von HCM bis zum Eingang neuer Daten per Internet als verbindlich zur Leistungsdurchführung verwendet. Hierbei auftretende Verzögerungen sind technisch bedingt und stellen keinen Mangel dar.
Dem Kunden ist bekannt, dass für alle Teilnehmer im Übertragungsweg des Internets in der Regel die Möglichkeit besteht, von in Übermittlung befindlichen Daten ohne Berechtigung Kenntnis zu erlangen. Dieses Risiko trägt der Kunde.
HCM weist gemäß § 33 BDSG darauf hin, dass personenbezogene Daten im Rahmen der Vertragsdurchführung gespeichert werden, und nicht an Dritte weitergeleitet werden. Ansonsten werden personenbezogene Daten nur erhoben, verarbeitet oder genutzt, sofern der Kunde einwilligt oder eine Rechtsvorschrift dies vorschreibt oder erlaubt. Durch den Abschluss des Vertrags mit HCM und die Zustimmung zu diesen Nutzungsbedingungen stimmt der Kunde der elektronischen Speicherung der Daten zu.

2. Service Level Agreement (SLA)

Kontaktmöglichkeiten
>> Standard: Ticketsystem
optional: Telefon, E-Mail
Klärungen: Webkonferenz

Zeitliche Verfügbarkeit des Support-Teams
>> Montag - Freitag, 8.00 - 17.00 Uhr

Antwortzeit auf Meldungen
>> Bis Mittag des Folgetages

Benachrichtigung des Kunden
>> Per E-Mail bei Störungen und geplanten Massnahmen

Recoveryzeit bei Absturz der Lösung
>> Bis Mittag des Folgetages (neu angelegte Vorgänge am Tag des Absturzes sind i.d.R. verloren)

Verfügbarkeit
>> Verfügbarkeit des Rechenzentrums 99%

3. Technische Daten der Cloudlösung

Adressierung
>>Kunde erhält eigene deutsche IP-Adresse, z.B. hcm-beschwerdemanagement-kundenname.de

Servertyp
>>Virtueller Server

Prozessoren
>>vCPU 4 Cores (nicht überbuchte dedizierte Prozessorcores)

Hauptspeicher
>>vMEM 8GB (nicht überbuchter dedizierter Arbeitsspeicher)

Festplatte
>>vHDD Single 80 GB (2 x 40 GB)

Betriebssystem
>>Windows Server

Datenbank
>> MS SQL Server Web Edition

Datenübertragungsmenge
>> unbegrenzt (fair use 1 TB)

Geschwindigkeit und Art
>> 2 x 1 Gbit

4. Optionen

Zugriffsschutz
>> VPN

Archivierung
>> Langzeitarchivierung der Daten bzw. Vorgänge

Datensicherheit
>> Echtzeit-Spiegelung des virtuellen Servers auf einem zweiten virtuellen Server

Server
>> Es kann ein dedizierter Server bereitgestellt werden

Prozessoren
>> Anderer Typ oder weitere CPU´s

Hauptspeicher
>> Pro GB

Festplatte
>> Pro GB

Schnittstellen
>> zu externen Systemen möglich

5. Nutzungsbedingungen

Die Nutzungsbedingungen entnehmen Sie bitte dem Dokument „Nutzungsbedingungen“