Datenschutz auf höchstem Niveau

hyperspace beachtet die Datenschutzbestimmungen der Bundesrepublik Deutschland und behandelt personengebundene Daten streng vertraulich und gibt diese nicht zu Werbezwecken an Dritte weiter.
Der Betrieb unserer Server erfolgt in Deutschland, die Daten werden innerhalb Deutschlands verarbeitet, es gilt deutsches Recht.

hyperspace Dimensions und hyperspace Franchise Manager sind mit dem Siegel „Software Hosted in Germany“ des Bundesverband IT-Mittelstand e.V. zertifiziert.

Hostway Deutschland GmbH ist durch das Bundesamt für Sicherheit in der Informationstechnik nach ISO 27001 „IT-Grundschutz“ zertifiziert (Zertifikats-Nr.: BSI-IGZ-0230-2016).

Gemeinsam mit unserem Rechenzentrumsbetreiber Hostway in Hannover treffen wir umfassende Maßnahmen auf dem aktuellen Stand der Technik für den Schutz der Daten, die Sie uns anvertraut haben:

Physische Sicherheit

Unsere Produktionsserver befinden sich im Hostway-Rechenzentrum in Hannover. Die physische Sicherheit unserer Server und Ihrer Daten wird u.a. durch folgende Maßnahmen rund um die Uhr gewährleistet: Identifikation aller im Rechenzentrum tätigen Personen, Zugang nur für berechtigte Personen nach vorheriger Anmeldung, ausfallsichere Stromversorgung, Temperaturregulierung im Datencenter, Brandschutzeinrichtungen sowie weitere Sicherungsfunktionen, die für einen sicheren Betrieb der Server sorgen und mit deren Hilfe Sicherheitsrisiken auf vorausschauende Weise erkannt werden.

Datenverschlüsselung

hyperspace setzt leistungsstarke Verschlüsselungsprodukte (SSL/TLS) namhafter Anbieter (z.B. VeriSign, Thawte) zum Schutz der Kundendaten und Kundenkommunikation ein. Das Schloss-Symbol im Browser zeigt an, dass die Daten während der Übertragung vollständig vor unautorisiertem Zugriff geschützt sind.

Benutzerauthentifizierung

Benutzer können nur mit einer gültigen Kombination aus Benutzername und Kennwort auf hyperspace Anwendungen zugreifen. Diese Angaben können zudem bei der Übertragung mit SSL verschlüsselt werden. Jeder Benutzer wird über eine verschlüsselte Sitzungs-ID eindeutig identifiziert. Um die Sicherheit zusätzlich zu erhöhen, ist die Sitzungsdauer zeitlich begrenzt und wird nach einer gewissen Zeit der Inaktivität automatisch beendet.

Backup

Eine tägliche, ortsfern ausgelagerte Datensicherung sorgt dafür, dass Ihre Daten selbst im Falle von Störungen oder Systemausfällen nicht verloren sind.

Passwortsicherheit

Das Passwort wird nicht in der Datenbank gespeichert, sondern nur der Hashwert des Passwortes, der zuvor zusätzlich mit einem SALT-String verfälscht wurde. Der SALT-String ist pro Userkonto unterschiedlich und wird mittels Triple-DES (DESede) erzeugt. Das Hashverfahren ist SHA-256.
Wenn ein User ein neues Passwort vergibt, wird durch einen farbigen Balken die Sicherheit des Passwortes visualisiert. Dabei werden Länge und Komplexität der eingegebenen Zeichenkette berücksichtigt.

Anwendungssicherheit

Das robuste Anwendungssicherheitsmodell verhindert, dass ein hyperspace-Kunde auf die Daten eines anderen Kunden zugreifen kann. Das Sicherheitsmodell wird bei jeder Anforderung neu angewendet und während der gesamten Benutzersitzung durchgesetzt.

Schutz gegen Cross-Site Scripting-Angriffe

Alle eingegebenen Benutzereingaben und URL-Parameter werden durch eine spezielle Prüfroutine auf Scripting-Angriffe geprüft und verdächtige Bestandteile vor der weiteren Verarbeitung entfernt.

Schutz gegen SQL-Injection-Angriffe

Eine Typprüfung der Variablen, die an SQL-Abfragen übergeben werden, verhindert wirkungsvoll SQL-Injection-Angriffe auf die Datenbank. Beim Login-Formular findet zusätzlich noch eine mehrfach gestaffelte Abfrage der Benutzerdaten statt.

Interne Systemsicherheit

Der Zugriff auf die Server wird durch Firewalls des Rechenzentrums und zusätzliche Firewall-Software auf den Hosting-Servern nach dem aktuellen Stand der Technik geschützt. Grundsätzlich sind auf unseren Servern nur solche Portadressen freigeschaltet, die für den Produktionsbetrieb unbedingt notwendig sind.

Betriebssystem

hyperspace gewährleistet eine hohe Sicherheit auf Betriebssystemebene, da für die Produktionsserver nur ein Minimum an Zugriffspunkten verwendet wird. Alle Betriebssystemkonten werden durch wirksame Kennwörter geschützt. Für alle Betriebssysteme werden regelmäßig die vom jeweiligen Hersteller empfohlenen Sicherheits-Patches installiert. Außerdem werden alle nicht erforderlichen Benutzer, Protokolle und Prozesse deaktiviert oder entfernt, um die Betriebssysteme noch weiter zu immunisieren.

Datensicherheit und Servermanagement

Alle Daten, die von einem Kunden in die hyperspace-Anwendung eingegeben werden, sind Eigentum dieses Kunden. Die Mitarbeiter und Entwickler von hyperspace haben keinen direkten Zugriff auf die Produktionsgeräte von hyperspace, es sei denn, dies ist für die Verwaltung, Wartung und Überwachung des Systems oder für Sicherungen unbedingt erforderlich. hyperspace Mitarbeiter und Vertragspartner sowie die Mitarbeiter des Rechenzentrums sind selbstverständlich auf das Datengeheimnis verpflichtet. Wartungsarbeiten an den Servern sind nur von ausgewählten hyperspace-Arbeitsplätzen aus möglich, die zudem besonders geschützt sind. Die Kommunikation zwischen Wartungsarbeitsplatz und Server wird verschlüsselt. Mitarbeiter des Rechenzentrums haben keinen Zugriff auf die Anwendungen der Kunden von hyperspace.

Entwicklungssicherheit

Alle Entwicklerarbeitsplätze werden von Virenschutz-Software und anderen Schutzprogrammen nach aktuellem Stand der Technik geschützt. Alle Änderungen an Softwaremodulen werden mithilfe einer serverbasierten Versionskontroll-Software verfolgt und dokumentiert. Alle Änderungen werden in speziellen Entwicklungssystemen vorgenommen und dann zuerst in Testsystemen geprüft, bevor sie in den Produktionssystemen implementiert werden. Externe Entwickler erhalten keinerlei Zugang zu Produktionssystemen, Kundenpasswörter oder Kundendaten und sind verpflichtet, für alle von Ihnen erstellten Programme und Programmteile entsprechende Testmodule zu erstellen, mit denen wir bei hyperspace die Programme auf modularer Ebene testen können.