Stand Jänner 2016

Detailinformationen gemäß § 25 TKG

zu den Allgemeinen Geschäftsbedingungen der i4a GmbH

Information gemäß § 25 Abs. 4 Z 2 lit e TKG 2003

Detailinformationen zu eingerichteten Verfahren, um den Datenverkehr zu messen und zu kontrollieren.

Die nachfolgenden Informationen beziehen sich auf jenen Teil des Netzes, über die öffentliche Internet Zugangsdienste bereitgestellt werden.

Zur Qualitätssicherung und Netzwerkplanung unserer Dienste werden regelmäßig Messungen des Datenverkehrs und der Systemausfallzeiten auf sämtlichen Netzhierarchien durchgeführt. Diese Daten, die lediglich aggregierte und damit anonyme Daten beinhalten, werden ausschließlich dazu verwendet, um Kapazitätsauslastungen und Ausfälle rechtzeitig zu erkennen und die Stabilität und Qualität des Netzes nachhaltig zu erhöhen. Die Erfassung dieser Daten hat keine Auswirkungen auf die Qualität der Services.

Information gemäß § 25 Abs. 4 Z 8 TKG 2003

Detailinformationen zu Maßnahmen, mit denen auf Sicherheits- oder Integritätsverletzungen reagiert werden kann.

Die i4a GmbH stellt sicher, dass die Sicherheit und die Integrität des Netzes dem jeweiligen Stand der Technik sowie den jeweiligen gesetzlichen Vorschriften entspricht und hat sämtliche dafür erforderlichen technischen und organisatorischen Maßnahmen im Unternehmen getroffen. Diese Maßnahmen sind in verbindlichen unternehmensinternen Sicherheitsrichtlinien festgehalten deren Einhaltung laufend überprüft wird.

Diese Maßnahmen umfassen insbesondere:

- Regelungen hinsichtlich der internen Organisation und Verantwortlichkeit für IT-Sicherheit
- Regelungen für Zugangsmanagement und Zugangskontrolle; Festlegung von Berechtigungsstufen für den physischen Zugang bzw. den Zugang zu Netzwerken und Anwendungen
- Regelmäßige Schulung unserer Mitarbeiter um das Sicherheitsbewusstsein zu schärfen
- Regelungen für den sicheren Umgang mit Benutzerkennwörtern
- Regelungen für die Vorgehensweise für neue und ausscheidende Mitarbeiter
- Regelungen hinsichtlich Datensicherheitsmaßnahmen
- Regelungen für die Netzwerksicherheit
- Regelmäßige Überprüfung unserer technischen Geräte auf mögliche Sicherheitsschwachstellen
- Ständige Aktualisierung der Antivirus- Software: Rund um die Uhr Kontrollen hinsichtlich neuer Updates
- Ständige Überprüfung der verwendeten Betriebssysteme ob Patches, Upgrades oder Hotfixes verfügbar sind.
- Regelungen für den Einsatz neuer Software; verpflichtende Tests vor dem Einsatz in der Produktionsumgebung
- Regelungen für das sichere Entfernen und Wiederverwenden von Geräten