Datenschutzrichtlinie der SCALTEL AG

SCALTEL AG
Buchenberger Str. 18
87448 Waltenhofen
Telefon: +49 831 540 54-0
Telefax: +49 831 540 54-109
datenschutz@scaltel.de

- nachfolgend SCALTEL AG genannt -
Vertretungsberechtigter Vorstand: Christian Skala (Vorsitzender), Joachim Skala
Aufsichtsratsvorsitzender: Alfons Hörmann

Präambel

Die SCALTEL AG, als datenverarbeitendes Unternehmen, unterliegt gemäß Bundesdatenschutzgesetz (BDSG) speziellen Verpflichtungen.
Um Kunden, Geschäftspartner und Lieferanten, aber auch Mitarbeiterinnen und Mitarbeitern ein besonders hohes Maß an Datenschutz zu gewährleisten, wird das Datenschutzkonzept der SCALTEL AG ständig überarbeitet und verbessert.

Datenschutzkonzept

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung, Grundsatz der Datenvermeidung und Datensparsamkeit, Schutz der Betroffenen

Gegenstand der SCALTEL AG ist der Vertrieb von Informations-Technologien.
Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der o. g. Zwecke.

Kundendaten, Mitarbeiterdaten sowie Daten von Lieferanten und ggf. von Interessenten werden erhoben, wenn dies zur Erfüllung der genannten Zwecke erforderlich sein sollte. Die SCALTEL AG unterwirft sich dem Grundsatz der Datensparsamkeit und erhebt, verarbeitet oder nutzt so wenig personenbezogene Daten wie möglich.

2. Bestellung eines Datenschutzbeauftragten

Die SCALTEL AG hat, gem. § 4f BDSG, Herrn Michael Fochtmann
als Datenschutzbeauftragten bestellt.

Herr Fochtmann ist für Sie wie folgt erreichbar

Herr Michael Fochtmann
Buchenberger Str. 18
87448 Waltenhofen
Telefon: +49 831 540 54-0
Telefax: +49 831 540 54-109

datenschutz@scaltel.de

3. Technische und organisatorische Maßnahmen

Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen technische und organisatorische Maßnahmen treffen, um den Bestimmungen des BDSG insbesondere dem §9 zu entsprechen.
Die Spezifizierung dieser Anforderungen ergibt sich aus der Anlage zu § 9 BDSG. Die SCALTEL AG erfüllt diesen Anspruch durch folgende Maßnahmen:

a) Zutrittskontrolle

Der Zugang zum Unternehmensgelände ist für Betriebsfremde nur während der allgemeinen Geschäftszeiten möglich. Zusätzlich zu Schutzzaun und Schiebetor wird das Gelände mit Videokameras und Infrarotmeldern überwacht. Weitere Zugänge zum Gebäude sind mit Zutrittskontrollsystemen gesichert. Jeder externe Besucher muss sich am Empfang anmelden und wird mit einem Besucherausweis versehen. Der Empfang führt den Besucher in ein Besprechungszimmer und verständigt den jeweiligen Gesprächspartner.
Die Besprechungen finden ausschließlich in den dafür vorgesehenen Besprechungs- und Schulungsräumen statt.
Firmenbesichtigungen / Rundgänge mit Neukunden sowie Präsentationen im Labor finden nur in Begleitung und nach Rücksprache und Kenntnisnahme durch den Abteilungsleiter statt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen.
Außerhalb der Arbeitszeiten erfolgt die Überwachung der Räumlichkeiten durch eine Alarmanlage sowie Videokameras. Alarmmeldungen werden durch einen externen Sicherheitsdienst nach einem festgelegten Interventionsplan überwacht und verfolgt.

b) Zugangskontrolle zu EDV-Systemen

Die Serverräume verfügen über weitere Zutrittskontrollsysteme und ermöglichen somit nur einigen wenigen dazu autorisierten Mitarbeiterinnen und Mitarbeitern den Zutritt.
Der Netzwerkzugriff wird über 802.1x geregelt. Unbefugten wird der Zugang zu Datenverarbeitungssystemen verweigert. Besucher haben die Möglichkeit über ein vom SCALTEL – Netzwerk getrenntes Gästenetzwerk Zugang zum Internet zu bekommen.
Das interne Netz ist über eine Firewall mit Intrusion Prevention Security (IPS) Funktion von der WAN-Seite (Internet) abgesichert. Die Verbindung zu den Niederlassungen sowie den Kunden erfolgt über einen VPN-Tunnel.

Alle PC-Systeme sind passwortgeschützt. Es gelten unternehmenseigene Passwortrichtlinien und eine maximale Laufzeit von 90 Tagen. Clientrechner müssen beim Verlassen des Arbeitsplatzes gesperrt werden, zusätzlich wird nach 15 Minuten Inaktivität jeder Rechner automatisch gesperrt.
Zentral verwaltete Virenscanner auf Client- und Serversystemen schützen
vor Malwareangriffen.

c) Zugriffskontrolle

Der Zugriff auf Netzwerkverzeichnisse, in denen personenbezogene Daten gespeichert werden, ist über Gruppenrichtlinien auf die jeweiligen Personen beschränkt, die Zugriff zur Ausübung der oben genannten Zwecke benötigen. Diese Personen müssen sich gegenüber dem System authentifizieren. Nach sechs fehlerhaften Anmeldeversuchen wird das Benutzerkonto automatisch gesperrt. Auf Mitarbeiterdaten hat ausschließlich die Personalabteilung Zugriff. Datenträger werden verschlossen aufbewahrt und sind somit nur für Personen mit entsprechender Berechtigung zugänglich.

d) Weitergabe Kontrolle

Die interne Nutzung von Internet und E-Mail ist über eine Dienstanweisung geregelt und die jeweils aktuellste Version steht den Mitarbeitern im Intranet zur Verfügung. Alle Mitarbeiter der SCALTEL AG haben eine Verpflichtungs-erklärung zur Wahrung des Datengeheimnisses und der Verschwiegenheit unterschrieben. Laptops mit Windows 7 sind AES Verschlüsselt (BitLocker) und somit vor dem Missbrauch durch Dritte geschützt. Kundeneinwahlen erfolgen grundsätzlich

verschlüsselt. Ausgediente oder defekte Datenträger werden zentral gesammelt und so vernichtet, dass sich nicht mehr rekonstruierbar sind.

e) Eingabekontrolle

Der Kreis der Nutzer ist durch die Rechtevergabe entsprechend eingeschränkt. Die Aktivitäten werden in einem Systemlog erfasst.

f) Auftragskontrolle

Bei der Vertragsgestaltung wird auf eine klare Abgrenzung der Kompetenzen und Pflichten von Auftraggeber und Auftragnehmer geachtet. Zu den getroffenen Sicherheitsvorkehrungen gehören die unter Verfügbarkeitskontrolle aufgeführten Maßnahmen.

Zum Abschluss jedes Projekts findet eine Kontrolle der ordnungsgemäßen Vertragsausführung statt.

g) Verfügbarkeitskontrolle

Die Rechenzentren der SCALTEL AG sind redundant aufgebaut.
Eine Brandmeldeanlage verhindert das unbemerkte Ausbrechen von Feuer, zusätzlich sind die Gebäudeteile durch Brandschutzabschnitte getrennt. Notfallpläne regeln die genaue Vorgehensweise zur Wiederherstellung nach einem Systemausfall. Tägliche Datensicherungen beugen Datenverlust vor.

h) Getrennte Verarbeitung personenbezogener Daten

Die erhobenen Daten werden über ein entsprechendes Berechtigungskonzept getrennt und der Zugriff eingeschränkt.
Bei Daten, die vom Kunden eingesehen werden können, ist ebenfalls durch ein Berechtigungskonzept sichergestellt, dass jeder Kunde nur Daten sehen kann, die ihn betreffen.

4. Unterbeauftragung

Sofern sonstige Dienstleister bzw. Unterauftragsnehmer der SCALTEL AG beauftragt werden und die Beauftragung den Umgang mit personenbezogenen Daten erforderlich macht, ist es unerlässlich, dass seitens des beauftragten Unternehmens eine unterzeichnete Datenschutzverpflichtungserklärung nach BDSG §11 vorliegt.
Sofern die Erteilung solcher Auftragsverhältnisse die Zustimmung eines Dritten erfordert, wird die SCALTEL AG diese Zustimmung über den Auftraggeber einholen.

5. Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen

Sämtliche Mitarbeiterinnen und Mitarbeiter wurden beim Eintritt in die Firma auf die Verpflichtungen zur Wahrung des Datengeheimnisses hingewiesen und bezeugten dies durch ihre Unterschrift.
Im Intranet findet sich zudem die aktuellste Version der IT Richtlinien der SCALTEL AG, die für jeden Mitarbeiter bindend ist.

6. Überprüfung durch Dritte

In regelmäßigen Abständen wird die SCALTEL AG durch einen Wirtschaftsprüfer und externe Zertifizierungsunternehmen im Rahmen von ISO 9001 Audits sowie ISO 20000 Audits überprüft.