

## **Informationen zur Umsetzung von Datenschutz und Datensicherheit bei der Aurenz GmbH**

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb betreiben wir unsere Aktivitäten in Übereinstimmung mit den geltenden Rechtsvorschriften sowie weiteren internen Regelungen zu Datenschutz und Informationssicherheit. Schon immer haben wir unsere Produkte datenschutzkonform entwickelt. Deshalb beschreiben wir im Folgenden grundlegende technische und organisatorische Maßnahmen, die die Aurenz GmbH unter anderem zum Schutz von Service- und Fernwartungsdienstleistungen umsetzt.

### **I. Pflichten zur Wahrung des Datenschutzes - Verpflichtung einzelner Mitarbeiter**

Jeder Mitarbeiter der Aurenz GmbH ist im Rahmen des Arbeitsvertrages zur Wahrung von Geschäfts- und Betriebsgeheimnissen verpflichtet.

Alle Mitarbeiter, die aufgrund ihrer Tätigkeit regelmäßig Zugang oder Zugriff zu Datenbeständen mit personenbezogenen Daten haben, werden zusätzlich schriftlich auf das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz (BDSG) verpflichtet.

Mitarbeiter, die mit Telekommunikationsdaten in Berührung kommen können, werden darüber hinaus zur Wahrung des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG) verpflichtet.

Um allen Mitarbeitern den sachgemäßen und rechtsicheren Umgang mit personenbezogenen und sensiblen Daten sowie deren Umsetzung in der Praxis, nahe zu bringen, werden sie vor Aufnahme ihrer Tätigkeit während einer persönlichen Schulung und dann in regelmäßigen Abständen durch Fachkräfte aus dem Datenschutzzumfeld eingewiesen.

### **II. Technische und organisatorische Maßnahmen gemäß BDSG**

Die Aurenz GmbH hat die im Bundesdatenschutzgesetz geforderten Maßnahmen (insbesondere zur Datensicherheit nach § 9 BDSG und Anlage) in einer Datenschutzerklärung festgeschrieben. Die Dokumentation ist nicht nur auf den Schutz personenbezogener Daten beschränkt, sondern kommt bei der Verarbeitung aller anfallender Daten, einschließlich der Daten Dritter wie Kunden, Lieferanten und Dienstleister zur Anwendung. Um den Anforderungen neuer rechtlicher und technischer Bedingungen gerecht zu werden, wird die Dokumentation stetig aktualisiert. Somit werden die Anforderungen zur Datensicherheit gemäß der Anlage (zu § 9 Satz 1) BDSG sichergestellt.

Der Datenschutzbeauftragte ist zentraler Ansprechpartner für das Thema Datenschutz und Informationssicherheit bei der Aurenz GmbH. Er berichtet regelmäßig direkt an die Geschäftsleitung.

### **III. Sicherstellung der besonderen Anforderungen bei Servicearbeiten sowie Fern-/ Remotezugriffen (nach § 11 Absatz (5) BDSG)**

Um die personenbezogenen Daten unserer Kunden bei Servicearbeiten sowie bei der Nutzung prozessunterstützender Tools und Systeme mittels Remotezugriff gegen unbeabsichtigte Veränderung oder Löschung, gegen unberechtigten Zugriff und Weitergabe sowie gegen Verlust zu schützen, hat die Aurenz GmbH mehrere ineinander greifende Sicherheitslösungen realisiert. In den folgenden Maßnahmen sind die Datenschutz- und Datensicherheitsmaßnahmen beschrieben:

## 1. Zutrittskontrolle

Der Zutritt zu Arbeitsplatzrechnern und Servern ist grundsätzlich verschlossen. Der Zutritt für Besucher wird durch eigenes Personal kontrolliert. Hierdurch wird der Zutritt der Berechtigten sicher gestellt. Die Sicherheitsanforderungen an Rechnerräume werden physikalisch sichergestellt.

## 2. Zugangskontrolle

Der Zugang zu Endgeräten von Mitarbeitern wird durch Betriebssystemkennung und ein persönliches Passwort geschützt.

Der Zugang von außen auf das Netz der Aurenz GmbH wird durch verschlüsselte Verbindungen sicher gestellt.

Firewallösungen schirmen das Netzwerk gegen unerlaubten Zugriff aus dem Internet ab. Verbindungen zu Kunden werden über VPN Gateways oder gesicherte Fernadministrationstools hergestellt. Zugriffe werden dokumentiert.

Mitarbeiter erhalten nur im Rahmen Ihrer Tätigkeit Zugriff auf die zur Vertragserfüllung notwendigen Systeme und Daten.

Die vom Kunden zur Authentifizierung eingerichteten und an die Aurenz GmbH übergebenen Zugangskennungen und Passwörter von kundeneigenen Systemen verlassen den Personenkreis der Berechtigten nicht. Sie werden in gesicherten Bereichen unserer IT-Systeme hinterlegt und sind nur dem Personenkreis zugänglich, der diese für die Erbringung der vereinbarten Dienstleistung zwingend benötigt.

## 3. Zugriffskontrolle

Der Zugriff auf die für die Vertragserfüllung notwendigen Daten wird innerhalb der Systeme und Applikationen durch ein entsprechendes Rollen- und Berechtigungskonzept umgesetzt.

## 4. Weitergabekontrolle

Die Weitergabe von personenbezogenen Daten an Unterauftragnehmer der Aurenz GmbH wird im Rahmen eines entsprechenden Vertrages mit dem Kunden festgelegt. Sie erfolgt stets zweckgebunden und über gesicherte Verbindungen. Personenbezogene Daten werden derzeit nur an Unterauftragnehmer mit Sitz innerhalb der EU/EWR übermittelt.

## 5. Eingabekontrolle

Die Eingabekontrolle wird über technische und organisatorische Maßnahmen dokumentiert. Bei Servicezugriffen werden Mitarbeiter, Partner, Kunde sowie Datum, Beginn und Ende mit Kurzbeschreibung der erbrachten Dienstleistung dokumentiert. Zusätzlich wird die Eingabekontrolle über Systemprotokolle dokumentiert.

## 6. Auftragskontrolle

Die Aurenz GmbH verwendet personenbezogene Daten nur für interne Zwecke im Rahmen der Kundenbeziehung. Eine Übermittlung an Dritte erfolgt ausschließlich unter Berücksichtigung vertraglicher und datenschutzrechtlicher Regelungen. Details zur Auftragskontrolle werden im Rahmen des jeweiligen Vertrages geregelt.

## 7. Verfügbarkeitskontrolle

Personenbezogene Daten werden sobald sie nicht mehr zu Bearbeitungszwecken erforderlich sind, zeitnah gelöscht. Aus gesetzlichen Gründen gilt zu beachten, dass bei jeder Löschung von Daten diese zunächst nur gesperrt und dann mit einer zeitlichen Verzögerung endgültig gelöscht werden können, um versehentliches Löschen oder evtl. vorsätzlicher Schädigungen vorzubeugen. Gleiches gilt für Daten, die zu einem Auftrag geführt haben bzw. zur Rückabwicklung eines Auftrages benötigt werden. Aus technischen Gründen werden Daten ggf. in Datensicherungsdateien und Spiegelungen von Diensten vorrätig gehalten. Solche Kopien werden ebenfalls ggf. erst mit einer technisch bedingten zeitlichen Verzögerung gelöscht.

## 8. Trennungskontrolle

Die Aurenz GmbH nutzt personenbezogene Daten nur für interne Zwecke im Rahmen des Auftrages oder der Kundenbeziehung. Die Daten werden entsprechend des Auftrages getrennt gespeichert. Alle Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Dienstleistungserbringung und zur Wahrung der Zweckbindung zu erheben, zu verarbeiten und zu nutzen.

### Hinweise

Die allgemeinen Beschreibungen in diesem Dokument enthalten keine detaillierten technischen und organisatorischen Maßnahmen. Diese werden im Einzelfall individuell gestaltet.

Spezifische Merkmale sind im Einzelfall bei Vertragsschluss zu klären.

Der Kunde wird durch die Aurenz GmbH unverzüglich informiert, wenn ein Verdacht auf Datenschutzverletzungen vorliegt.