GRUNDREGELN DES DATENSCHUTZES IM SINNE DES TECHNISCH-ORGANISATORISCHEN DATENSCHUTZES

Hiermit bekennen wir uns zur Einführung, Umsetzung und Aufrechterhaltung der nachfolgenden Grundregeln des Datenschutzes im Sinne des technisch-organisatorischen Datenschutzes:

Zutrittskontrolle:
Unbefugte erhalten keinen Zutritt zu Datenverarbeitungsanlagen, mit denen Personenbezogene Daten verarbeitet werden, erhalten. Dies realsieren wir durch:

- Festlegung von Sicherungsbereichen
- Festlegung von befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung)
- Festlegung von Besucherregelungen
- Sicherung von Gebäuden und Räumen
- Anwesenheitsaufzeichnungen

Zugangskontrolle:
Nur Befugte Personen erhalten Zugang zu Datenverarbeitungsanlagen erhalten. Zu diesem Zweck sind DV-Anlagen grundsätzlich mit Zugangskennungen zu schützen. Nachfolgende Hinweise müssen beachtet werden:

- Nutzerkennungen, d.h. Nutzername und Passwort sind an den jeweiligen Nutzer gebunden und dürfen nicht weiter gegeben werden - ein Vorstoß gegen dieses Gebot ist mehr, als lediglich ein Fahrlässigkeitsdelikt und zieht im Schadensfall arbeitsrechtliche Maßnahmen und eventuell einen Strafantrag nach sich
- Passwörter müssen mindestens 6 Zeichen lang sein, sowie Sonderzeichen und Ziffern enthalten
- bei eventuellem Bekanntwerden des Passwortes muss dieses umgehend geändert werden

Zugriffskontrolle:
Berechtigte Personen, die sich mit ihrer Nutzerkennung ordnungsgemäß am DV-System identifiziert haben, besitzen entsprechend ihrer Nutzerrechte differenzierte und damit abgestufte Berechtigungen in den jeweiligen Software-Systemen. DerVersuch, sich weitere, nicht vergebene Nutzerrechte zu erschleichen, ist eine Straftat und zieht arbeitsrechtliche und strafrechtliche Konsequenzen nach sich.

Weitergabekontrolle:
Personenbezogene Daten und vertrauliche dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden. Soll die Exaktheit und Originalität des Dokumentes für den Empfänger nachvollziehbar sein, empfiehlt sich die Verwendung der digitalen Signatur. Der Umgang mit externen Datenträgern, wie z.B. USB-Sticks, externe Festplatten, SD-Speicherkarten u.ä. muss mit großer Sorgfalt erfolgen. Personenbezogene und vertrauliche Inhalte sollen verschlüsselt sein. Die Weitergabe

oder elektronische Übermittlung personenbezogener und vertraulicher Daten und Datenträger muss nachvollziehbar sein.

Eingabekontrolle:
Über die Werkzeuge der Nutzerverwaltung und der damit verbundenen Rechteverwaltung muss nachvollziebar sein, wer Neueingaben, Änderungen oder das Löschen personenbezogener und vertraulicher Informationen veranlasst hat. Deshalb wird an dieser Stelle nochmals auf das hohe Risiko der Weitergabe von Nutzerkennungen hingewiesen. Verantwortlich bleibt in jedem Falle der angemeldete Nutzer, nicht der geduldete Fremdnutzer im Vertretungsfalle.

Auftragskontrolle:
Bei personenbezogener Datenverarbeitung im Auftrag (z.B. Fremdwartung von Datenverarbeitungseinrichtungen, mit denen personenbezogene Informationen verarbeitet werden oder Entsorgung von Papier mit vertraulichen oder personenbezogenen Inhalten durch Fremdfirmen) müssen entsprechende vertragliche Regelungen getroffen sein, um die Tätigkeit dieser externen Auftragnehmer transparent zu halten.

Verfügbarkeitskontrolle:
Personenbezogene und andere vertrauliche Informationen müssen derart abgelegt werden, dass ein Verlust nicht möglich ist oder, dass im Falle eines Verlustes eine Rekonstruktion der Daten, mit einem vertretbaren technisch-organisatorischen Aufwand, möglich ist. Deshalb sind lokale Datenablagen nicht als hinreichend sicher einzustufen. Nur zentrale Ressourcen können hinreichend gesichert und im Schadensfall wieder hergestellt werden.

Prinzip der Zweckbindung:
Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden. Die Verwendung derartiger Daten in Verbunddateien (Nutzung eines ursprünglichen Datenbestandes auch für andere Zwecke) muss innerbetrieblich definiert und festgeschrieben sein.