**Datenschutz-Richtlinien der Stadtwerke Velbert GmbH für Lieferanten und sonstige Auftragnehmer**

Um die IT-Infrastruktur vor Störungen zu schützen und die Sicherheit der in ihr verarbeiteten, gespeicherten und übertragenen Informationen zu gewährleisten, werden Lieferanten und sonstige Auftragnehmer, die Zugriff auf IT-Systeme der Stadtwerke Velbert GmbH haben, zwingend auf nachfolgende Regelungen verpflichtet:

- Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, ist untersagt.
- Ebenfalls untersagt ist das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten.
- Alle in der IT-Infrastruktur eingesetzte Hard- und Software wird vor ihrem Einsatz erst nach Prüfung durch den IT-Verantwortlichen der Stadtwerke Velbert GmbH freigegeben.
- Das eigenmächtige Herunterladen von Software sowie die Installation oder Verwendung nicht freigegebener Hard- und Software ist den Lieferanten oder sonstigen Auftragnehmern nicht gestattet.
- Der Zugriff auf das Internet oder auf Netzwerke die nicht vom Unternehmen betrieben werden, erfolgt grundsätzlich nur über die vom Unternehmen speziell dafür bereitgestellten Zugänge.
- Zugangskennungen für die Nutzung der IT-Infrastruktur (wie z.B. Passwörter) sind von einem Lieferanten oder sonstigen Auftragnehmer geheim zu halten und dürfen grundsätzlich nicht an Dritte weitergegeben werden. Auch innerhalb der jeweiligen Organisation des Lieferanten oder sonstigen Auftragnehmers ist dieser verpflichtet, die Daten vor anderen Beschäftigten des Auftragnehmers geheim zu halten. Ausnahmen hiervon können gemacht werden, wenn die Leistungen des Auftragnehmers von einem Team von Personen für die Stadtwerke Velbert GmbH durchgeführt werden.
- Die private Nutzung von IT-Systemen der Stadtwerke Velbert GmbH ist jedem Lieferanten oder Auftragnehmer untersagt.
- Bei einem Einsatz von IT-Dienstleistern sind stets folgende Punkte zu berücksichtigen: IT-Systeme des Dienstleisters müssen über grundlegende Sicherheitsmaßnahmen verfügen:
- Das IT-System muss ausreichend vor Schadsoftware gesichert sein. Es ist ein Virenscanner zu verwenden, der eine tagesaktuelle Versorgung mit Updates von Virendefinitionen gewährleistet. Der Virenscanner muss permanent aktiviert sein.
- Betriebssysteme auf den IT-Systemen müssen auf dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters sein. Es sind nur Betriebssysteme zu verwenden, die vom Hersteller noch unterstützt und gepflegt werden („Support“).

**Sanktionen**

Für Verstöße der Auftragnehmer gegen die jeweils vereinbarten Pflichten im Zusammenhang mit Datenschutz und Informationssicherheit behalten wir uns Sanktionsmöglichkeiten vor.