Gesellschaft / Behörde _____

Name des Verantwortlichen _____

Straße _____

PLZ / Ort _____

Vertraulichkeitserklärung

1. Die oben genannte Gesellschaft / Behörde ist verpflichtet, über alle Informationen, die ihr im Zusammenhang mit ihrer Tätigkeit bei der Verkehrsbetriebe Peine-Salzgitter GmbH (VPS) bekannt werden, Stillschweigen zu bewahren, gleichgültig ob es sich dabei um VPS selbst oder deren Geschäftsverbindungen handelt.
2. Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die
    a. die oben genannte Gesellschaft / Behörde nachweislich von Dritten erhalten hat oder erhält,
    b. allgemein bekannt sind,
    c. deren Bekanntgabe VPS schriftlich zugestimmt hat.
3. Bei Einschaltung Dritter hat die oben genannte Gesellschaft / Behörde deren Verpflichtung zur Verschwiegenheit sicherzustellen.
4. Erhaltene Geschäfts- und Betriebsunterlagen dürfen nur im Rahmen der betrieblichen Erfordernisse und der urheberrechtlichen Bestimmungen vervielfältigt werden.
5. Die oben genannte Gesellschaft / Behörde hat die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG zu berücksichtigen (siehe Anlage).

Verpflichtung auf das Datengeheimnis

Die oben genannte Gesellschaft / Behörde wird wie folgt auf das Datengeheimnis nach Maßgabe des § 5 BDSG verpflichtet und auf die Strafbarkeit von Verstößen hingewiesen:

1. Die oben genannte Gesellschaft / Behörde verpflichtet sich, unbeschadet sonstiger betrieblicher Geheimhaltungspflichten, das Datengeheimnis zu wahren.
2. Die oben genannte Gesellschaft / Behörde ist befugt, ihr anvertraute personenbezogene Daten nur im Rahmen der mit ihr geschlossenen Vereinbarung zu verarbeiten.
3. Verstöße können nach § 43 ff BDSG und anderer einschlägiger Rechtsvorschriften mit Geld- oder Freiheitsstrafe geahndet werden.

Diese Pflicht besteht auch nach Beendigung des Vertragsverhältnisses mit VPS.

Ort, Datum

Unterschrift des Verantwortlichen / (Klarschrift)

1 Kopie an bDSB (Abt. ZA - Herr Ludwig)

1. Zutrittskontrolle → *Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.*
Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insb. auch zur Legitimation der Berechtigten:

- ☐ Zutrittskontrolle (Ausweisleser, Magnetkarte, Chipkarte
  → zu beachten: § 6c BDSG (Mobile personenbezogenen Speicher- und Verarbeitungsmedien)
- ☐ Schlüssel / Schlüsselvergabe
- ☐ Werkschutz, Pförtner
- ☐ Protokollierung der Zutritte / Abgänge
- ☐ Überwachungseinrichtungen (Alarmanlage, Video- /Fernsehmonitor
  → zu beachten: § 6b BDSG Beobachtung öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen)
- ☐ Türsicherung (elektrische Türöffner usw.)
- ☐ Festlegung der zutrittsberechtigten Personen
- ☐ Einrichtung von Sicherheitszonen u -bereichen

2. Zugangskontrolle → *Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.*
Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ☐ Einrichtung eines Benutzerstammsatzes pro User
- ☐ Absicherung der DV-Systeme und Netzwerke gegen Zugänge von außen
- ☐ Protokollierung der Zugänge
- ☐ Verschlüsselung von Datenträgern
- ☐ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßige Kennwortänderung)
- ☐ Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- ☐ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- ☐ Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System

3. Zugriffskontrolle →*Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*
Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- ☐ Berechtigungskonzepte (z.B. Profile, Rollen, Transaktionen)
- ☐ Regelmäßige Kontrolle der Gültigkeit der zugewiesenen Berechtigungen
- ☐ Festlegung der Zugriffsrechte (z.B. Lesen, Ändern, Löschen, Auswerten, Administrieren)
- ☐ Festlegung der personellen Zuständigkeiten
- ☐ Protokollierung der Zugriffe

4. Weitergabekontrolle →*Der Schutz personenbezogener Daten bei Weitergabe ist zu gewährleisten.*

- ☐ Verschlüsselung
- ☐ Elektronische Signatur
- ☐ Tunnelverbindung
- ☐ Protokollierung bei Weitergabe
- ☐ Virtual Private Network (VPN)
- ☐ Festlegung der Übermittlungswege und Datenempfänger
- ☐ Transportsicherung (z.B. verschlossener Versand, Kennwortschutz bei Dateiübertragung)

5. Eingabekontrolle →*Die Nachvollziehbarkeit der Datenverwaltung und –pflege ist zu gewährleisten.*

- ☐ Protokollierung der Eingabe
- ☐ Festlegung der Zuständigkeiten für Eingabe

6. Auftragskontrolle →*Die weisungsgemäße Auftragsdatenverarbeitung sowie die Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind zu gewährleisten.*

- ☐ Festlegung der Kriterien zur Auswahl des Auftragnehmers
- ☐ Regelmäßige Kontrolle der Vertragsausführung
- ☐ Eindeutige Vertragsgestaltung

7. Verfügbarkeitskontrolle →*Die Daten sind gegen Zerstörung oder Verlust zu schützen.*

- ☐ Notfallplan (z.B. USV)
- ☐ Virenschutz
- ☐ Getrennte Aufbewahrung
- ☐ Spiegeln von Festplatten
- ☐ Regelmäßige Datensicherung (Backup-Verfahren)
- ☐ Regelmäßige Durchführung einer Risiko- und Schwachstellenanalyse bezogen auf Hard- und Software

8. Trennungskontrolle →*Daten, die zu verschiedenen Zwecken erhoben wurden, sind getrennt zu verarbeiten.*

- ☐ Funktionstrennung / Produktion / Test
- ☐ Aufteilung in mehrere Mandanten